مقدمة في أمن الشبكات

Net Work Security

الدكتور

مروان العبد محمد أبو زعنونة

المهندس

علاء الدين الصويتي

الأستاذ

حاتم مبارك

INFORMATION SECURITY



مقدمة في امن الشبكات

Network Security

رقم الإيداع لدى دائرة المكتبة الوطنية
(٢٠٠٩/١٢/٥٢٣٩)

٠٠٥.٨
أبو زعنونة ، مروان العبد
مقدمة في أمن الشبكات/مروان العبد محمد أبو زعنونة
علاء الدين محمد الصويتي،حاتم مبارك
عمان: دار المعتز للنشر والتوزيع،٢٠٠٩
ر.أ (٢٠٠٩/١٢/٥٢٣٩)
//الواصفات /أمن الحاسوب//الجرائم الحاسوبية//الشبكات//الحاسوبية/

* أعدت دائرة المكتبة الوطنية بيانات الفهرسة والتصنيف الأولية
* يتحمل المؤلف كامل المسؤلية القانونية عن محتوى مصنفة ولا يعبّر هذا المصنف عن رأي دائرة المكتبة الوطنية أو اي جهة حكومية أخرى.

الطبعة الأولى
2010م - 1431هـ



دار المعتز للنشر والتوزيع
عمان - وسط البلد - مجمع الفحيص التجاري
تلفاكس: ٤٦٢٠٩٩٠ ٦ ٩٦٢+ ص.ب: ١٨٤٠٣٤ عمان: ١١١١٨ الأردن
e-mail:daralmuotaz@yahoo.com

مقدمة في أمن الشبكات

Network Security

د. مروان العبد محمد أبو زعنونة
م. علاء الدين محمد الصويتي
أ. حاتم مبارك

الطبعة الأولى
٢٠١٠م – ١٤٣١هـ

فهرس

الوحدة الأولى

أساسيات تأمين أجهزة الحاسبات

المقدمة

لم يكن هناك قلق مع بدايات شبكة الإنترنت تجاه" جرائم" يمكن أن تنتهك على الشبكة ، وذلك نظراً لمحدودية مستخدميها علاوة على كونها مقصورة على فئة معينة من المستخدمين وهم الباحثين ومنسوبي الجامعات. لهذا فالشبكة ليست آمنة في تصميمها وبناءها. لكن مع توسع استخدام الشبكة ودخول جميع فئات المجتمع إلى قائمة المستخدمين بدأت تظهر جرائم على الشبكة ازدادت مع الوقت وتعددت صورها وأشكالها.

بعد التقدم والتطور الذي حصل في عالم الأمن (Security)، وبعد تطور أساليب المخترقين في عملياتهم وتنوعها Man-IN-THE-Middle و Sniffing والـ Relaying والكثير غيرها ،، كان لا بد من إيجاد طريقة أمنه لتخطي هذه الأمور وخصوصا في الأمور الحساسة كالتجارة الالكترونية وعمليات كشف الحسابات عن طريق الانترنت وغيرها ، فكان لابد من طريقه لتامين ذلك.

إن شبكة الإنترنت كشبكة معلوماتية ينطبق عليها النموذج المعروف لأمن المعلومات لأهمية تأمين الأجهزة بما فيها من معلومات بالأبعاد الثلاثة وهي :

١- سرية المعلومات:

وذلك يعني ضمان حفظ المعلومات المخزنة في أجهزة الحاسبات أو المنقولة عبر الشبكة وعدم الإطلاع عليها إلا من قبل الأشخاص المخولين بذلك.

٢- سلامة المعلومات:

يتمثل ذلك في ضمان عدم تغيير المعلومات المخزنة على أجهزة الحاسب أو المنقولة عبر الشبكة إلا من قبل الأشخاص المخولين بذلك.

٣- وجود المعلومات:

وذلك يتمثل في عدم حذف المعلومات المخزنة على أجهزة الحاسب إلا من قبل الأشخاص المخولين بذلك.

إن جرائم الإنترنت ليست محصورة في هذا النموذج ، بل ظهرت جرائم لها صور أخرى متعددة تختلف باختلاف الهدف المباشر في الجريمة.

أهم الأهداف المقصودة في تلك الجرائم :

١.١- المعلومات:

يشمل ذلك سرقة أو تغيير أو حذف المعلومات ، ويرتبط هذا الهدف بشكل مباشر بالنموذج الذي سبق ذكره.

١.٢- الأجهزة:

ويشمل ذلك تعطيلها أو تخريبها.

١.٣- الأشخاص أو الجهات:

تهدف فئة كبيرة من الجرائم على شبكة الإنترنت أشخاص أو جهات بشكل مباشر كالتهديد أو الابتزاز. علماً بأن الجرائم التي تكون أهدافها

المباشرة هي المعلومات أو الأجهزة تهدف بشكل غير مباشر إلى الأشخاص المعنيين أو الجهات المعنية بتلك المعلومات أو الأجهزة. بقي أن نذكر أن هناك جرائم متعلقة بالإنترنت تشترك في طبيعتها مع جرائم التخريب أو السرقة التقليدية ، كأن يقوم المجرمون بسرقة أجهزة الحاسب المرتبطة بالإنترنت أو تدميرها مباشرة أو تدمير وسائل الاتصال كالأسلاك والأطباق الفضائية وغيرها. حيث يستخدم المجرمون أسلحة" تقليدية" ابتداء من المشارط والسكاكين وحتى عبوات متفجرة ، وكمثال لهذا الصنف من الجرائم قام مشغل أجهزة في إحدى الشركات الأمريكية بصب بنزين على أجهزة شركة منافسة وذلك لإحراقها حيث دمر مركز الحاسب الآلي الخاص بتلك الشركة المنافسة برمته.

٢ـ بعض جرائم الإنترنت التي تؤدي إلى إتلاف الأجهزة وفقد المعلومات في الشبكة :

٢.١- صناعة ونشر الفيروسات

وهي أكثر جرائم الإنترنت انتشارا وتأثيرا. إن الفيروسات كما هو معلوم ليست وليدة الإنترنت فقد أشار إلى مفهوم فيروس الحاسب العالم الرياضي المعروف فون نيومن في منتصف الأربعينات الميلادية. لم تكن الإنترنت الوسيلة الأكثر استخداما في نشر وتوزيع الفيروسات إلا في السنوات الخمس الأخيرة ، حيث أصبحت الإنترنت وسيلة فعالة وسريعة في نشر الفيروسات. ولا يخفى على الكثير سرعة توغل ما

يسمى بـ "الدودة الحمراء" حيث استطاعت خلال أقل من تسع ساعات اقتحام ما يقرب من ربع مليون جهاز في 19 يوليو ٢٠٠١م. إن الهدف المباشر للفيروسات هي المعلومات المخزنة على الأجهزة المقتحمة حيث تقوم بتغييرها أو حذفها أو سرقتها و نقلها إلى أجهزة أخرى.

٢.٢- الاختراقات:

تتمثل في الدخول غير المصرح به إلى أجهزة أو شبكات حاسب آلي. إن جل عمليات الاختراقات (أو محاولات الاختراقات) تتم من خلال برامج متوفرة على الإنترنت يمكن لمن له خبرات تقنية متواضعة أن يستخدمها لشن هجماته على أجهزة الغير، وهنا تكمن الخطورة .

تختلف الأهداف المباشرة للاختراقات، فقد تكون المعلومات هي الهدف المباشر حيث يسعى المخترق لتغيير أو سرقة أو إزالة معلومات معينة . وقد يكون الجهاز هو الهدف المباشر بغض النظر عن المعلومات المخزنة عليه، كأن يقوم المخترق بعمليته بقصد إبراز قدراته "الإختراقيه" أو لإثبات وجود ثغرات في الجهاز المخترق .

من أكثر الأجهزة المستهدفة في هذا النوع من الجرائم هي تلك التي تستضيف المواقع على الإنترنت، حيث يتم تحريف المعلومات الموجودة على الموقع أو ما يسمى بتغيير وجه الموقع (Defacing). إن استهداف هذا النوع من الأجهزة يعود إلى عدة أسباب من أهمها كثرة وجود هذه

الأجهزة على الشبكة ، وسرعة انتشار الخبر حول اختراق ذلك الجهاز خاصة إذا كان يضم مواقع معروفة.

٢.٣- تعطيل الأجهزة:

كثر مؤخراً ارتكاب مثل هذه العمليات ، حيث يقوم مرتكبوها بتعطيل أجهزة أو شبكات عن تأدية عملها بدون أن تتم عملية اختراق فعلية لتلك الأجهزة. تتم عملية التعطيل بإرسال عدد هائل من الرسائل بطرق فنية معينة إلى الأجهزة أو الشبكات المراد تعطيلها الأمر الذي يعيقها عن تأدية عملها.

من أشهر الأمثلة على هذا النوع من الجرائم تلك التي تقوم بتعطيل الأجهزة المستضيفة للمواقع على الشبكة. إن الأسباب وراء استهداف هذا النوع من الأجهزة تماثل أسباب استهدافها في جرائم الاختراقات والتي سبق ذكرها في "ثانيا".

جميع الجرائم التي ذكرناها تستهدف بشكل مباشر معلومات أو أجهزة وشبكات حاسبات. أما جرائم الإنترنت التي تستهدف جهات سواء كانوا أفراداً أو مؤسسات ، ففيما يلي عرض لبعضها :

٢.٤- انتحال الشخصية :

هي جريمة الألفية الجديدة كما سماها بعض المختصين في أمن المعلومات وذلك نظراً لسرعة انتشار ارتكابها خاصة في الأوساط التجارية. تتمثل هذه الجريمة في استخدام هوية شخصية أخرى بطريقة غير شرعية ،

وتهدف إما لغرض الاستفادة من مكانة تلك الهوية (أي هوية الضحية) أو لإخفاء هوية شخصية المجرم لتسهيل ارتكابه جرائم أخرى. إن ارتكاب هذه الجريمة على شبكة الإنترنت أمر سهل وهذه من أكبر سلبيات الإنترنت الأمنية . وللتغلب على هذه المشكلة ، فقد بدأت كثير من المعاملات الحساسة على شبكة الإنترنت كالتجارية في الاعتماد على وسائل متينة لتوثيق الهوية كالتوقيع الرقمي والتي تجعل من الصعب ارتكاب هذه الجريمة .

٢.٥- المضايقة والملاحقة :

تتم جرائم الملاحقة على شبكة الإنترنت غالباً باستخدام البريد الإلكتروني أو وسائل الحوارات الآنية المختلفة على الشبكة. تشمل الملاحقة رسائل تهديد وتخويف ومضايقة. تتفق جرائم الملاحقة على شبكة الإنترنت مع مثيلاتها خارج الشبكة في الأهداف والتي تتمثل في الرغبة في التحكم في الضحية . تتميز جرائم المضايقة والملاحقة على الإنترنت بسهولة إمكانية المجرم في إخفاء هويته علاوة على تعدد وسهولة وسائل الاتصال عبر الشبكة ، الأمر الذي ساعد في تفشي هذه الجريمة. من المهم الإشارة إلى أن كون طبيعة جريمة الملاحقة على شبكة الإنترنت لا تتطلب اتصال مادي بين المجرم والضحية لا يعني بأي حال من الأحوال قلة خطورتها. فقدرة المجرم على إخفاء هويته تساعده على التمادي في جريمته والتي قد تفضي به إلى تصرفات عنف مادية علاوة

على الآثار السلبية النفسية على الضحية .

٢.٦- التغرير والاستدراج:

غالب ضحايا هذا النوع من الجرائم هم صغار السن من مستخدمي الشبكة. حيث يوهم المجرمون ضحاياهم برغبتهم في تكوين علاقة صداقة على الإنترنت والتي قد تتطور إلى التقاء مادي بين الطرفين. إن مجرمي التغرير والاستدراج على شبكة الإنترنت يمكن لهم أن يتجاوزوا الحدود السياسية فقد يكون المجرم في بلد والضحية في بلد آخر. وكون معظم الضحايا هم من صغار السن ، فإن كثير من الحوادث لا يتم الإبلاغ عنها ، حيث لا يدرك كثير من الضحايا أنهم قد ُغرر بهم .

٢.٧- التشهير وتشويه السمعة:

يقوم المجرم بنشر معلومات قد تكون سرية أو مضللة أو مغلوطة عن ضحيته، والذي قد يكون فرداً أو مجتمع أو دين أو مؤسسة تجارية أو سياسية. تتعدد الوسائل المستخدمة في هذا النوع من الجرائم، لكن في مقدمة قائمة هذه الوسائل إنشاء موقع على الشبكة يحوي المعلومات المطلوب نشرها أو إرسال هذه المعلومات عبر القوائم البريدية إلى أعداد كبيرة من المستخدمين.

٢.٨- النصب والاحتيال :

أصبحت الإنترنت مجالاً رحباً لمن له سلع أو خدمات تجارية يريد أن يقدمها ، وبوسائل غير مسبوقة كاستخدام البريد الإلكتروني أو عرضها على موقع على الشبكة أو عن طريق ساحات الحوار. ومن الطبيعي

أن يُساء استخدام هذه الوسائل في عمليات نصب واحتيال. ولعل القارئ الكريم الذي يستخدم البريد الإلكتروني بشكل مستمر تصله رسائل بريدية من هذا النوع. إن كثيراً من صور النصب والاحتيال التي يتعرض لها الناس في حياتهم اليومية لها مثيل على شبكة الإنترنت مثل بيع سلع أو خدمات وهمية ، أو المساهمة في مشاريع استثمارية وهمية أو سرقة معلومات البطاقات الائتمانية واستخدامها. وتتصدر المزادات العامة على البضائع عمليات النصب والاحتيال على الإنترنت. إن ما يميز عمليات النصب والاحتيال على الإنترنت عن مثيلاتها في الحياة اليومية هي سرعة قدرة مرتكبها على الاختفاء والتلاشي .

٢.٩- **الهجوم** Attacks :

يقسم الهجوم إلى أربعة أقسام وهي:

١. **هجوم التصنت على الرسائل:**Interception Attacks

وفكره عمل هذا الهجوم: أن المهاجم يراقب الاتصال بين المرسل والمستقبل للحصول على المعلومات السرية وهو ما يسمى بالتصنت على الاتصال .(Eavesdropping)

٢. **هجوم الإيقاف** :Interruption Attacks

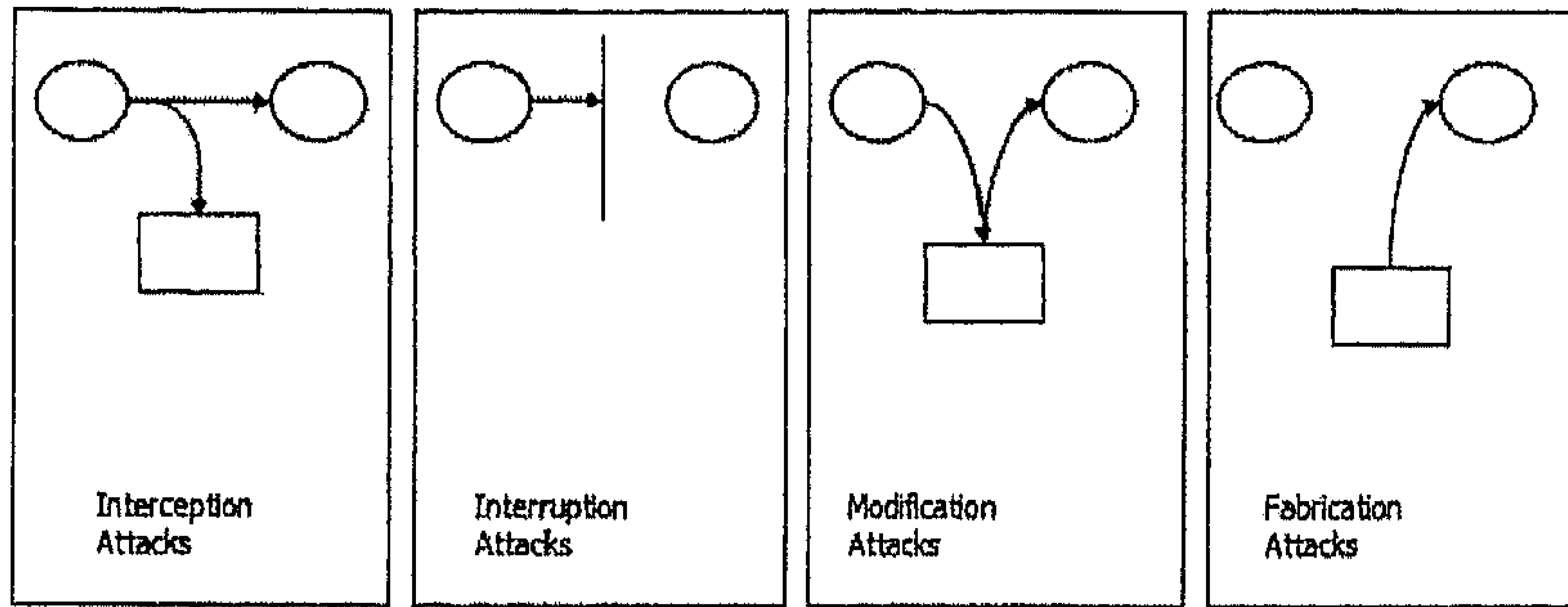
وهذا النوع يعتمد على قطع قناة الاتصال لإيقاف الرسالة أو البيانات من الوصول إلى المستقبل وهو ما يسمى أيضا برفض الخدمة (Denial of service).

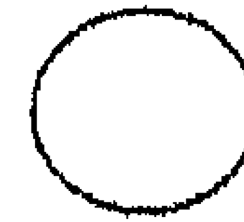
٣. هجوم يعدل على محتوى الرسالة: Modification Attacks

وهنا يتدخل المهاجم بين المرسل والمستقبل (يعتبر وسيط بين المرسل والمستقبل) وعندما تصل إلى الـ Attacker فإنه يقوم بتغيير محتوى الرسالة ومن ثم إرسالها إلى المستقبل أوالمستقبل طبعا لا يعلم بتعديل الرسالة من قبل الـAttacker.

٤. الهجوم المزور أو المفبرك : Fabrication Attacks

وهنا يرسل المهاجم رسالة مفادها انه صديقه ويطلب منه معلومات أو كلمات سرية خاصة بالشركة مثلا.



 المرسل والمستقل المخولين في دخول الأنظمة(Authorized entity)

 المهاجم Attacker أو الغير مخول لهم (Unauthorized entity)

وبعد أن أخذنا مقدمة عن أمن المعلومات أوالجرائم التي من الواجب الحذر منها، لابد لنا من معرفة :

١ – تعريف الخطر وأقسامه.

2 – الإجراءات المضادة عند حدوث الخطر Countermeasures.

٣– كيفية إدارة الخطر و احتمال حدوثه.

٣ـ تعريف الخطر الخطر وأقسامه :

الخطر (Risk) : هو أنه يوجد على الأرجح تهديد يمكن استغلاله ، وبالتالي إذا استغل ذلك التهديد يمكن أن نطلق عليه ثغرة (Vulnerability)، حيث أنه يوجد ثغرة أمنية في تلك المنظمة .

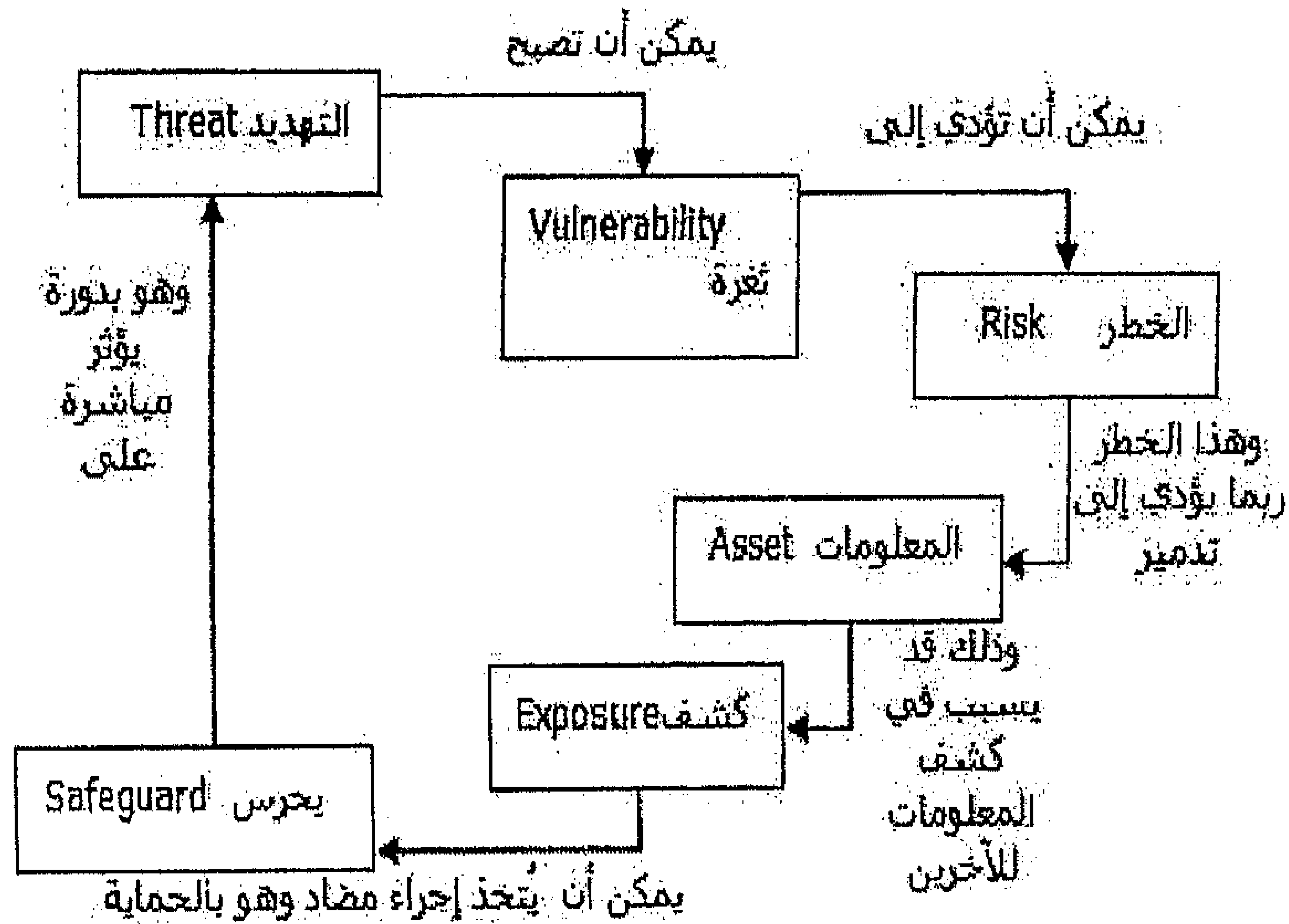
ومن هذا التعريف يمكن أن نقسم الخطر Risk إلى قسمين رئيسيين هما

3.1 - (Threat) **التهديد**:

وهو عملية المحاولة إلى الوصول إلى المعلومات السرية الخاصة بالمنظمة.

3.2- (Vulnerabilities) **الثغرات**: وهي أنه يوجد ضعف في المنظمة يستطيع المهاجم Attacker الدخول من خلالها .

وهناك مكونات أخرى للخطر وهي كما يوضح الشكل التالي :



٣.١ .الثغرات Vulnerabilities

تتكون من نوعين وهما:

- **تحصين تقني** Technical Vulnerability: إذا كان التحصين ضعيفا واستغل الضعف من قبل المهاجم Attacker يعرف هذا الهجوم بما يسمى بالهجوم التقني.

- تحصين غير تقني Administrative Vulnerability : وهو ما يسمى بالهجوم الغير تقني أو هجوم الهندسة الاجتماعية social engineering Attack.

٣.٢- التهديد Threat

هناك ثلاث مكونات أساسيه للتهديد وهي Threat :

- **الهدف**Target:

وهي المعلومات المراد سرقتها .

- **الطريقة** Agent

:أو العميل وهي الأشياء المكونة والمنشأة للتهديد .

- **الحدث** Event:

وهي نوعية التأثير لوضعية التهديد

ولنتحدث عن كل منهم بالتفصيل:

٣.٢.١- **الهدف** Target:

وهي المعلومات الخاصة بالمنظمة ويمكن للمهاجم Attacker بعمل الآتي على كل من :

- Confidentiality **الخصوصية:**

وذلك بكشف المعلومات السرية للآخرين.

- Integrity **سلامه المعلومات:**

يمكنه تغيير المعلومات الخاصة بالمنظمة.

- Availability **التواجد:**

بواسطة رفض الخدمة عن طريق Dos

- Accountability **قابلية محاسبة المهاجم:**

لكي لا يحاسب المهاجم Attacker فإنه يقوم بإخفاء الهجوم على سبيل المثال تغيير سجل الأحداث. (Events logs)

٢.٢.٣- **طريقة العميل** Agent:

لابد من توفر ثلاث سمات:

- Access to the target **الوصول إلى الهدف:**

وقد يكون وصول مباشر Direct (أي أن لدية حساب دخول على النظام وقد يكون غير مباشر Indirect (وذلك بالدخول عن طريق وسيط)

- Knowledge about the target **معلومات عن الضحية.**
- Motivation **الدوافع أو أسباب الهجوم.**

٢.٢.٣- **الأحداث** EventS :

وهي تكون بطرق عديدة من أهمها إساءة الدخول المخول Authorized وغير المخول UnauthorizeD إلى المعلومات أو النظام. وإما عن طريق وضع أكواد خبيثة MaliciouS (تروجونات أو فيروسات) في الأنظمة.

٤- طرق فقد المعلومات وإتلاف محتويات الأجهزة في الشبكات :

إن من أهم أسباب تلف المعلومات وإتلاف محتويات الأجهزة في الشبكات تأتي من خلال اختراقات الأشخاص.

٤.١ - تعريف الاختراق و دوافعه و أنواعه و آثاره:

الاختراق بشكل عام هو القدرة على الوصول لهدف معين بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاص بالهدف وبطبيعة الحال هي سمة سيئة يتسم بها المخترق لقدرته على دخول أجهزة الآخرين عنوه ودون رغبة منهم وحتى دون علم منهم بغض النظر عن الأضرار الجسيمة التي قد يحدثها سواء.

بأجهزتهم الشخصية أو بنفسياتهم عند سحبة ملفات وصور تخصهم وحدهم .

٤.١.١ - دوافع الاختراق :

- لم تنتشر هذه الظاهرة لمجرد العبث وإن كان العبث وقضاء وقت الفراغ من أبرز العوامل التي ساهمت في تطورها وبروزها الي عالم الوجود .

وقد أجمل من المؤلفين المتخصصين في هذا المجال الدوافع الرئيسية للاختراق ثلاث نقاط على النحو التالي:

4.1.1.1 - الدافع السياسي والعسكري :

مما لاشك فيه أن التطور العلمي والتقني أديا إلي الاعتماد بشكل شبة كامل على أنظمة الكمبيوتر في أغلب الاحتياجات التقنية والمعلوماتية. فمنذ الحرب الباردة والصراع المعلوماتي و التجسسي بين الدولتين العظميين آنذاك على أشده. ومع بروز مناطق جديدة للصراع في العالم وتغير الطبيعة المعلوماتية للأنظمة والدول ، أصبح الاعتماد كليا على الحاسوب الآلي وعن طريقه اصبح الاختراق من اجل الحصول على معلومات سياسية وعسكرية واقتصادية مسألة أكثر أهمية .

4.1.1.2 -الدافع التجاري :

من المعروف أن الشركات التجارية الكبرى تعيش هي أيضا فيما بينها حربا مستعرة الكوكا كولا والبيبسي كولا على سبيل المثال) وقد بينت الدراسات الحديثة أن عددا من كبريات الشركات التجارية يجرى عليها أكثر من خمسين محاولة اختراق لشبكاتها كل يوم .

٤.١.١.٣ - **الدافع الفردي :**

بدأت أولى محاولات الاختراق الفردية بين طلاب الجامعات بالولايات المتحدة كنوع من التباهي بالنجاح في اختراق أجهزة شخصية لأصدقائهم ومعارفهم وما لبثت أن تحولت تلك الظاهرة إلي تحدي فيما بينهم في اختراق الأنظمة بالشركات ثم بمواقع الانترنت. ولا يقتصر الدافع على الأفراد فقط بل توجد مجموعات ونقابات أشبه ما تكون بالأندية وليست بذات أهداف تجارية .

بعض الأفراد بشركات كبرى بالولايات المتحدة ممن كانوا يعملون مبرمجين ومحللي نظم تم تسريحهم من أعمالهم للفائض الزائد بالعمالة فصبوا جم غضبهم على أنظمة شركاتهم السابقة مقتحميها ومخربين لكل ما تقع أيديهم علية من معلومات حساسة بقصد الانتقام . وفي المقابل هناك هاكرز محترفين تم القبض عليهم بالولايات المتحدة وبعد التفاوض معهم تم تعيينهم بوكالة المخابرات الأمريكية (CIA) وبمكتب التحقيقات الفيدرالي (FBI) وتركزت معظم مهماتهم في مطاردة الهاكرز وتحديد مواقعهم لإرشاد الشرطة إليهم .

٤.٢ - **أنواع الاختراق :**

يمكن تقسيم الاختراق من حيث الطريقة المستخدمة إلي ثلاثة أقسام :

١.٢.٤ - اختراق المزودات أو الأجهزة الرئيسية للشركات والمؤسسات أو الجهات الحكومية وذلك باختراق الجدران النارية التي عادة توضع

لحمايتها وغالبا ما يتم ذلك باستخدام المحاكاة Spoofing وهو مصطلح يطلق على عملية انتحال شخصية للدخول إلي النظام حيث أن حزم الـ IP تحتوي على عناوين للمرسل والمرسل إليه وهذه العناوين ينظر إليها على أنها عناوين مقبولة وسارية المفعول من قبل البرامج وأجهزة الشبكة . ومن خلال طريقة تعرف بمسارات المصدر Source Routingفإن حزم الـ IP قد تم إعطائها شكلا تبدو معه وكأنها قادمة من كمبيوتر معين بينما هي في حقيقة الأمر ليست قادمة منه وعلى ذلك فإن النظام إذا وثق بهوية عنوان مصدر الحزمة فإنه يكون بذلك قد حوكي (خدع) وهذه الطريقة هي ذاتها التي نجح بها مخترقي الهوتميل في الولوج إلى معلومات النظام قبل فترة قريبة من الزمان .

٤.٢.٢- اختراق الأجهزة الشخصية والعبث بما تحويه من معلومات

وهي طريقة للأسف شائعة لسذاجة أصحاب الأجهزة الشخصية من جانب ولسهولة تعلم برامج الاختراقات وتعددها من جانب آخر .

٤.٢.٣- التعرض للبيانات أثناء انتقالها والتعرف على شيفرتها إن كانت مشفرة وهذه الطريقة تستخدم في كشف أرقام بطاقات الائتمان وكشف الأرقام السرية للبطاقات البنكية ATM وفي هذا السياق نحذر هنا من أمرين لا يتم الاهتمام بهما بشكل جدي وهما عدم كشف أرقام بطاقات الأئتمان لمواقع التجارة الالكترونية إلا بعد التأكد بالتزام تلك المواقع بمبدأ الأمان . أما الأمر الثاني فبقدر ما هو ذو أهمية أمنية عالية

إلا أنه لا يؤخذ مأخذ الجديه . فالبعض عندما يستخدم بطاقة السحب الألي من آلات البنوك النقدية ATM لا ينتظر خروج السند الصغير المرفق بعملية السحب أو انه يلقي به في اقرب سلة للمهملات دون أن يكلف نفسه عناء تمزيقه جيدا . ولو نظرنا إلي ذلك المستند سنجد أرقاما تتكون من عدة خانات طويلة هي بالنسبة لنا ليست بذات أهمية ولكننا لو أدركنا بأن تلك الأرقام ما هي في حقيقة الأمر إلا انعكاس للشريط الممغنط الظاهر بالجهة الخلفية لبطاقة الـ ATMوهذا الشريط هو حلقة الوصل بيننا وبين رصيدنا بالبنك الذي من خلاله تتم عملية السحب النقدي لأدركنا أهمية التخلص من المستند الصغير بطريقة مضمونه ونقصد بالضمان هنا عدم تركها الهاكر محترف يمكنه استخراج رقم الحساب البنكي بل والتعرف على الأرقام السرية للبطاقة البنكية .

٤.٣ -آثار الاختراق:

4.3.1 - تغيير الصفحة الرئيسية لموقع الويب كما حدث لموقع فلسطيني مختص بالقدس حيث غير بعض الشباب الإسرائيلي الصور الخاصة بالقدس إلي صور تتعلق بالديانة اليهودية بعد عملية اختراق مخطط لهاأو أيضاً كما حصل موقع قناة الجزيرة الفضائية مؤخراً إثر عرضها لصور الأسرى الأمريكيين على شاشتها و موقعها فقامت جهة ما باختراق موقعها و تعطيلها لأكثر من يوم كامل و غيرت الصفحة الرئيسة له بصورة العلم الأمريكي.

٤.٣.٢- السطو بقصد الكسب المادي كتحويل حسابات البنوك او الحصول على خدمات مادية أو أي معلومات ذات مكاسب مادية كأرقام بطاقات الائتمان والأرقام السرية الخاصة ببطاقات الـATM.

إقتناص كلمات السر التي يستخدمها الشخص للحصول على خدمات مختلفة كالدخول إلى الانترنت حيث يلاحظ الضحية ان ساعاته تنتهي دون أن يستخدمها وكذلك انتحال شخصية في منتديات الحوار أ أو الاستيلاء على بريد شخص ما.

٤.٤- آلية الاختراق :

يعتمد الاختراق على السيطرة عن بعد Remote وهي لا تتم الا بوجود عاملين مهمين الأول البرنامج المسيطر ويعرف بالعميل Client والثاني الخادم Server الذي يقوم بتسهيل عملية الاختراق ذاتها .

وبعبارة أخرى لابد من توفر برنامج على كل من جهازي المخترق والضحية ففي جهاز الضحية يوجد برنامج الخادم وفي جهاز المخترق يوجد برنامج العميل .

تختلف طرق اختراق الأجهزة والنظم باختلاف وسائل الاختراق ، ولكنها جميعا تعتمد على فكرة توفر اتصال عن بعد بين جهازي الضحية والذي يزرع به الخادم (server) الخاص بالمخترق ، وجهاز المخترق على الطرف الأخر حيث يوجد برنامج المستفيد او العميل Client و ذلك عن طريق أربعة أساليب :

٤.٤.١ - ملفات أحصنة طروادة :

لتحقيق نظرية الاختراق لابد من توفر بريمج تجسسي يتم إرساله و زرعه من قبل المستفيد في جهاز الضحية ويعرف بالملف اللاصق ويسمى الصامت أحياناً (وهو ملف باتش patch صغير الحجم مهمته الأساسية المبيت بجهاز الضحية الخادم) وهو حلقة الوصل بينه وبين المخترق (المستفيد) .

٤.٤.١.١ - كيفية الإرسال والاستقبال :

تقوم الفكرة هنا على إرسال ملف باتش صغير هذا الملف يعرف باسم حصان طروادة لأنه يقوم بمقام الحصان الخشبي الشهير في الأسطورة المعروفة الذي ترك أمام الحصن وحين ادخله إليه الناس خرج من داخلة الغزاة فتمكنوا من السيطرة و الاستيلاء على الحصن . ملفنا الصغير الفتاك هذا ربما يكون أكثر خبثا من الحصان الخشبي بالرواية لأنه حالما يدخل لجهاز الضحية يغير من هيئته فلو فرضنا بأن اسمه Bush.exe وحذرنا منه صديق فأننا سنجده يحمل اسما آخرا بعد يوم أو يومين .

لهذا السبب تكمن خطورة أحصنه طروادة فهي من جانب تدخل للأجهزة في صمت وهدوء ، ويصعب اكتشافها من جانب آخر في حالة عدم وجود برنامج جيد مضاد للفيروسات .

لا تعتبر أحصنة طروادة فيروسات وإن كانت برامج مضادات الفيروسات تعتبرها كذلك فهي بالمقام الأول ملفات تجسس ويمكن أن

يسيطر من خلالها المستفيد سيطرة تامه على جهاز الضحية عن بعد وتكمن خطورتها في كونها لا تصدر أية علامات تدل على وجودها بجهاز الخادم .

٤.٤.١.١.١ - كيفية الإرسال :

تتم عملية إرسال بريمجات التجسس بعدة طرق من أشهرها البريد الالكتروني حيث يقوم الضحية بفتح المرفقات المرسلة ضمن رسالة غير معروفة المصدر فيجد به برنامج الباتش المرسل فيظنه برنامجا مفيدا فيفتحه او أنه يفتحه من عامل الفضول ليجده لا يعمل بعد فتحة فيتجاهلة ظانا بأنه معطوب ويهمل الموضوع بينما في ذلك الوقت يكون المخترق قد وضع قدمه الأولى بداخل الجهاز (يقوم بعض الأشخاص بحذف الملف مباشرة عند اكتشافهم بأنه لا يعمل ولكن يكون قد فات الأوان لأن ملف الباتش من هذا النوع يعمل فورا بعد فتحة وإن تم حذفه.

هناك طرق أخرى لزرع أحصنه طروادة غير البريد الالكتروني كانتقاله عبر المحادثة من خلال برنامج الـ ICQ وكذلك عن طريق إنزال بعض البرامج من احد المواقع الغير موثوق بها . كذلك يمكن إعادة تكوين حصان طروادة من خلال الماكرو الموجودة ببرامج معالجات النصوص .

٤.٤.١.١.٢- كيفية الاستقبال :

عند زرع ملف الباتش في جهاز الضحية (الخادم) فأنه يقوم مباشرة بالاتجاه إلى ملف تسجيل النظام Registry لأنه يؤدي ثلاثة أمور رئيسية في كل مرة يتم فيها تشغيل الجهاز :

١- فتح بوابة او منفذ ليتم من خلالها الاتصالل .

٢- تحديث نفسه وجمع المعلومات المحدثة بجهاز الضحية استعدادا لإرسالها للمخترق فيما بعد .

٣- وتحديث بيانات المخترق (المستفيد) في الطرف الأخر .تكون المهمة الرئيسية لملف الباتش فور زرعة مباشرة فتح منفذ اتصال داخل الجهاز المصاب تمكن برامج المستفيد (برامج الاختراقات) من النفوذ. كما أنه يقوم بعملية التجسس بتسجيل كل ما يحدث بجهاز الضحية أو انه يقوم بعمل أشياء أخرى حسب ما يطلبه منه المستفيد كتحريك الماوس أو فتح باب محرك السي دي وكل ذلك يتم عن بعد .

٤.٤.١.١.٢.١- بوابات الأتصال Ports :

يتم الاتصال بين الجهازين عبر بوابات ports أو منافذ اتصال وقد يظن البعض بأنها منافذ مادية في إمكانه رؤيتها كمنافذ الطابعة والفأرة ولكنها في واقع الأمر جزء من الذاكرة له عنوان معين يتعرف علية الجهاز بأنه منطقة اتصال يتم عبره إرسال واستقبال البيانات ويمكن استخدام عدد كبير من المنافذ للاتصال وعددها يزيد عن ٦٥٠٠٠ يميز كل منفذ عن

الآخر رقمه فمثلا المنفذ رقم ١٠٠١ يمكن إجراء اتصال عن طريقة وفي تقس اللحظة يتم استخدام المنفذ رقم 2001 لإجراء اتصال آخر .

٢.٢.١.١.٤.٤- التواصل :

قلنا بأن المخترق قد تمكن من وضع قدمه الأولى بداخل جهاز الضحية بعد زرع ملف الباتش به ورغم خطورة وجود هذا الملف بجهاز الضحية فأنه يبقى في حالة خمول طالما لم يطلب منه المخترق التحرك فهو مجرد خادم ينفذ ما يصدر له من أوامر ولكن بدونه لا يتمكن المخترق من السيطرة على جهاز الضحية عن بعد.

وحتى يتم له ذلك، فإن على المخترق بناء حلقة وصل متينة بينه وبين الخادم عن طريق برامج خاصة تعرف ببرامج الاختراق .

من جانب آخر تبقى أحصنة طروادة عديمة الفائدة إن لم يتمكن المخترق من التعامل معها وهي تفقد ميزتها الخطرة حالما يتم اكتشافها والتخلص منها . وهناك عامل ممتاز يساهم في تحقيق هذه الميزة فبرامج مضادات الفيروسات الجيدة تكتشف ملفات الباتش الحاملة لأحصنة طروادة وتمنعها من الدخول للأجهزة لهذا يؤكد كل من له إلمام بالمعلوماتية أن تزود دائما الأجهزة الشخصية ببرامج مضادات الفيروسات وتحديثها بين الحين والأخر لأنها الخطوة الأولى للوقاية من الاختراقات ، كذلك علينا أن نتعود على عدم تمكين عامل الفضول من الولوج إلى أنفسنا فل انفتح أية مرفقات للبريد الالكتروني مجهول

المصدر مهما كانت المغريات .

٤.٤.٢-**عن طريق** الـ IP Address :

ذكرت بأن ملفات الباتش الحاملة لأحصنة طروادة هي حلقة الوصل بين المخترق والضحية ، ولكن في واقع الأمر فإن ملفات الباتش ليست إلا طريقة واحدة لتحقيق التواصل . عند اتصالك بالانترنت تكون معرض لكشف الكثير من المعلومات عنك كعنوان جهازك وموقعه ومزود الخدمة الخاص بك وتسجيل كثير من تحركاتك على الشبكة .ولا تتعجب كثيرا حين تعلم بأن كثيرا من المواقع التي تزورها تفتح سجلا خاصا بك يتضمن عنوان الموقع الذي جئت منه IP Address ونوع الكمبيوتر والمتصفح الذي استخدمته بل وحتى نوع معالج جهازك وسرعته ومواصفات شاشاتك وتفاصيل كثيرة .

مبدئيا عنوانك الخاص بالانترنت Internet Protocol أو IP يكشف الكثير عنك فكل جهاز متصل بالشبكة يكون له رقم معين خاص به يعرف باسم الـ -IP Address وكل عنوان لموقع على الانترنت يترجم إلى IP Address الخاص بمزود الخدمة وباختصار يكون الـ IP كرقم هوية خاص بكل من يعمل على الانترنت. حينما يتمكن مخترق محترف من معرفة رقم الـ IP الخاص بالضحية فأنه من خلاله يتمكن من الولوج إلى الجهاز والسيطرة عليه خلال الفترة التي يكون فيها الضحية متصلا بالشبكة فقط ، ولكن هذا الخيار لا يخدم

المخترق كثيرا لأن السيرفر الخاص بمزود الخدمة يقوم بتغيير رقم الـ IP الخاص بالمشترك تلقائيا عند كل عملية دخول للشبكة . يمكنك أن تجرب ذلك بنفسك بالطريقة التالية :

أثناء اتصالك بالشبكة ومن قائمة إبداء أختر تشغيل واكتب الأمر التالي في المستطيل الظاهر winipcfg : سيظهر لك عنوان الـ IP اكتبه في ورقة صغيرة واقطع اتصالك . أعد الاتصال مرة أخرى بالشبكة وقم بالأجراء السابق ستجد أن

عنوان الـ IP الخاص بك قد تغير .

٤.٤.٣- عن طريق الكوكي Cookie :

يمكن أيضا تحقيق التواصل للاختراق عن طريق الكوكي Cookie وهي عبارة عن ملف صغير تضعه بعض المواقع التي يزورها المستخدم على قرصه الصلب .

هذا الملف به آليات تمكن الموقع الذي يتبع له جمع وتخزين بعض البيانات عن الجهاز وعدد المرات التي زار المستخدم فيها الموقع كما وأنها تسرع عمليات نقل البيانات بين جهاز المستخدم والموقع فالهدف الأساسي منها هو تجاري ولكنه يساء استخدامه من قبل بعض المبرمجين المتمرسين بلغة الجافا Java فهذه اللغة لديها قدرات عالية للتعمق أكثر لداخل الأجهزة والحصول على معلومات أكثر عن المستخدم.

لا يفضل منع الكوكيز كليا ولكن يمكن فلترتها من خلال المتصفح أو ببعض البرامج كالـ . (Guard Dog)

وبعد فإن آلية الاختراق تتم مبدئيا بوضع بريمج الخادم بجهاز الضحية ويتم الاتصال به عبر المنفذ port الذي فتحة للمستفيد (المخترق) في الطرف الأخر ولكن حلقة الوصل هذه تنقصها المعابر وهي البرامج المخصصة للاختراق وهذه الأخيرة.

٤.٤.٤ التجسس:

يظن بعض مستخدمي إنترنت، وخاصة المبتدئين منهم، أن لا أحد يستطيع اكتشاف ماذا يفعلون على الإنترنت :المواقع التي يزورونها..
المعلومات التي يقدمونها أثناء التسجيل في بعض المواقع، أو الشراء..
الحوارات التي يشاركون فيها ضمن المنتديات أو في غرف الدردشة..
الرسائل التي يكتبونها للمجموعات الإخبارية news groups
الكلمات والعبارات التي ينقبون عنها باستخدام محركات البحث..
الملفات التي يجلبونها..

لكن، من هو الجهة التي تصلك بالإنترنت، وهي إما مزود خدمات إنترنت الرئيسي ISP ، الذي تشترك معه، أو كمبيوتر مؤسستك، إذا كانت تتصل بإنترنت عن طريق خط خاص مؤجر leased line .

٤.٤.٤.١ - تخترق خصوصيتك في الشبكة من جهتين :

- مزودك بخدمة الاتصال بإنترنت ISP ، وهو اختراق يمكن أن يكون شاملاً.

- المواقع التي تزورها، ومنتديات الحوار التي تشارك فيها، أياً كان نوعها، وهو اختراق جزئي، لكنه خطر، أحياناً.

٤.٤.٤.٢ - ماذا يسجل مزود خدمات إنترنت عنك ؟

يمكن لمزود خدمات إنترنت، من الناحية النظرية، أن يكتشف كل أفعالك عندما تتصل بالشبكة، ويشمل ذلك، عناوين المواقع التي زرتها، ومتى كان ذلك، والصفحات التي اطلعت عليها، والملفات التي جلبتها، والكلمات التي بحثت عنها، والحوارات التي شاركت فيها، والبريد الإلكتروني الذي أرسلته واستقبلته، وفواتير الشراء التي ملأتها، والخدمات التي اشتركت بها. لكن، تختلف من الناحية الفعلية، كمية المعلومات التي يجمعها مزود خدمات إنترنت عنك، باختلاف التقنيات والبرمجيات التي يستخدمها. فإذا لم يكن مزود الخدمة يستخدم مزودات بروكسي (تتسلم وتفلتر كل طلباتك)، وبرمجيات تحسس الحزم "packet sniffer"تحلل حركة المرور بتفصيل كبير)، فقد لا يسجل عنك، سوى بياناتك الشخصية، ورقم IP الخاص بالكمبيوتر المتصل، وتاريخ وزمن اتصالك بالشبكة، وانفصالك عنها. أما إذا كان اتصالك يمر عبر "بروكسي"، فترتبط مستوى التفصيلات بالبرمجيات التي

يستخدمها مزود الخدمة، والتي يمكن أن تصل في حدها الأقصى، إلى المستوى النظري، الذي أشرنا إليه سابقاً. وينطبق ما ذكرناه، في حال كان اتصالك يتم عبر خط خاص مؤجر، للمؤسسة التي تعمل فيها.

أما الأخبار الطيبة لمستخدمي إنترنت، فهي أن معظم مزودي خدمات إنترنت لا يطلعون على السجلات، ما لم يطلب منهم ذلك بأمر رسمي من الجهات المسؤولية عن تطبيق القانون، وهو أمر نادر الحدوث. تبقى إمكانية التطفل على أفعال المشتركين قائمة، لكنها تتطلب جهوداً كبيرة، ووقتاً طويلاً، بالإضافة إلى أن معظم مزودي خدمات إنترنت غير مستعدين للمخاطرة بسرية المشتركين، وخسارة بعضهم. ولا يهتمون، لهذا السبب، بمراقبة المشتركين، بدلالة أنهم يرسلون رسائل البريد الصادر، بأسرع ما يمكن، لتحرير المساحات التي يشغلها على الأقراص الصلبة. ويحذفون البريد الإلكتروني الوارد، بسرعة، بعد أن يجلبه مستخدم إنترنت إلى كمبيوتره الخاص.

٤.٤.٤.٣- ماذا يسجل الموقع الذي تزوره عنك؟

عندما تتجول في حواري إنترنت، تترك أثار أقدامك في كل مكان تزوره. فالموقع الذي تمر به، يفتح سجلاً خاصاً بك، يتضمن عنوان الموقع الذي جئت منه، نوع الكمبيوتر والمتصفح الذي تستخدمه وعنوان IP الدائم، أو المتغير، للكمبيوتر الذي تتصل منه. ويمكن تحت ظروف معينة، أن يتمكن الموقع من الحصول على عنوان بريدك

الإلكتروني، واسمك الحقيقي. ويقول بعض الخبراء، أنه يمكن باستخدام بريمجات جافا، أو جافا سيكريب، أو أكتيف إكس، سرقة عنوان بريدك الإلكتروني، وبعض المعلومات الأخرى عنك، على الرغم من أن هذا العمل غير قانوني (تستطيع شل عمل جافا في إكسبلورر ٣.٢، من خلال الأوامر View ، ثم Options ، ثم Advanced ، وإزالة علامتي الاختيار من مربعي Enable Java JIT compiler، و enable Java Logging. من خلال الأوامر Options، ثم Network Preferences ، ثم Languages ، وإزالة علامتي الاختيار من مربعي Enable Java ، و enable (JavaScript

وتقدم أنت، معلوماتك الشخصية، عندما تملأ قسيمة الاشتراك في خدمات أحد المواقع. وننصحك في هذه الحالة، بالتأكد أولاً، من أن هذا الموقع "محترم"، ولن يسرب هذه المعلومات إلى جهات أخرى، قبل أن تقدم له هذه المعلومات.

تضع معظم مواقع ويب، عندما تزورها، ملفاً صغيراً على القرص الصلب لكمبيوترك، يسمى "كوكي Cookie " أو ملف الارتباط بهدف جمع بعض المعلومات عنك، وهو مفيد أحياناً، خاصة إذا كان الموقع يتطلب منك إدخال كلمة مرور تخولك بزيارته. ففي هذه الحالة لن تضطر في كل زيارة لإدخال تلك الكلمة، إذ سيتمكن الموقع من

اكتشافها بنفسه عن طريق "الكوكي"، الذي وضعه على قرصك الصلب، في الزيارة الأولى. لكن، يرى الكثير من المستخدمين في ذلك انتهاكاً لخصوصياتهم أثناء التصفح، خاصة عندما يراقب "الكوكي" تحركاتك ضمن الموقع. إذا كنت لا ترغب أن يسجل الآخرون "كوكيز" على قرصك الصلب، بهدف جمع بعض المعلومات عنك، فبإمكانك تجهيز المتصفح الذي تستخدمه، بحيث يطلب موافقتك، قبل أن يحفظ أي "كوكي"، على قرصك الصلب (تستطيع إجراء ذلك في المتصفح إكسبلورر ٣.٠٢، من خلال الأوامر ViеW ، ثمOptionS ، ثم Advanced، ووضع علامة الاختيار في مربع Warn before accepting “cookies”. وفي المتصفح نافيجيتور ٣.٠، من خلال الأوامرOptionS ، ثم Network Preferences ، ثم Protocols، وإزالة علامة الاختيار من مربع Accepting a Cookie). والأفضل أن تستخدم برامج، مثلeSafe Protect ، وGuard Dog، تحلل رموز الكوكي، وتعلمك ما إذا كان مفيداً أم لا، ثم نصحك بقبوله أو حذفه، بناء على ذلك التحليل.

تتمثل أكبر المخاطر التي قد تواجهها، في ما تكتبه ضمن المجموعات الإخبارية news groupS إذ تدخل رسائلك ضمن أرشيف www.dejanews.comحيث يمكن لأي شخص الاطلاع عليها، الآن، وربما بعد ٢٠ سنة، أيضاً. قد تشارك، عندما تكون شاباً في بعض

المجموعات الإخبارية غير المناسبة، وتكتب آراءً طائشة، لكن، عليك أن تعلم أن ما خطته يداك، قد يبقى إلى الأبد، وربما يطلع عليه أحفادك، أو جهات أخرى! وقد يستخدم يوماً كسلاح ضدك.

٥- مصادر تهديد الخصوصية و الإزعاج

5.1 - المتطفلين و المتجسسين على بريدك الإلكتروني

كثير من الناس مصابون بمرض التجسس على الغير و ينشأ معهم حب التتبع لخصوصيات الناس و هذه مشكلة مصاب بها بعض الناس منذ قديم الأزل و الى يومنا هذا وهم يتمكنون من ذلك بعدة طرق منها :

- برامج التجسس وهي كثيرة و متنوعة و متوفرة بالأسواق أو عن طريق الإنترنت .

- تخمين كلمات العبور السهلة التي قد يستخدمها الأصدقاء كاسم الدولة أو المدينة التي ولدت بها أو اسم المدرسة .

- استخدام برامج مخصصة للوصول إلى كلمات العبور وهي عبارة عن برامج تمكن مستخدمها من تجريب عدة آلاف من الكلمات السرية المنطقية و الشائعة لبن الناس وبذلك يمكن لها أن تصيب في بعض الأحيان.

كما يتمكن كل من يستطيعون الوصول الى جهازك في المكتب أو المنزل من الزملاء أو الأهل أو الأصدقاء من التطفل على رسائلك باستخدام بعض الخصائص المتوفرة في متصفحك و منها:

٥.١.١ - خاصية الرجوع للخلف في المتصفح:

- استخدام خاصية تذكر اسم المستخدم وكلمة العبور.
- استخدام خاصية الإكمال الالى للاسم و فراغات النماذج .
- استخدام خاصية تذكر الصفحات التي تقوم بزيارتها .

٥.٢ - المزعجين و المحولين

وهي عادة الشركات و المواقع التي تحصل على عنوان بريدك الإلكتروني و تقوم بتبادل هذه العناوين فيما بينهم أو تقوم ببيع هذه العناوين و كذلك يقوم بعض الأفراد بجمع هذه العناوين للقيام بإزعاج الآخرين أو لغرض بيعها لأحد الشركات و قد انتشرت مؤخرا رسائل باللغة العربية تحكي قصص محزنة لأطفال أو كبار تعرضوا لحوادث شخصية أو حوادث سير (طبعا تأليف في تأليف) و يطلب منك صاحب الرسالة بأن تساعد ذلك الطفل المسكين و القيام بإرسال الرسالة إلى كل من تعرف و من لا تعرف!! فتقوم بالعمل نيابة عنه بينما يقوم هو بجمع العناوين و تكوين ثروة من العناوين يقوم ببيعها أو يكون قد أرسل معها فيروس أو برنامج تجسس أو برنامج للتحكم و تعطيل المواقع وأنت لا تعلم عنها كما انتشرت في الآونة الأخيرة رسالة تحتوي على معلومات عن أحد مكونات (الشامبو و أنها تسبب السرطان) و يذكر فيها منتج معين ويمدح فيه بينما يذم في بقية الأنواع و يطلب منك أخبار كل الأصدقاء و المعارف عن طريق تحويل الرسالة و طبعا كل ذلك

الكلام ليس له أساس من الصحة و الهدف منه هو جمع العناوين أو التسويق الخاص بهم.

٦- الحماية :

تم تطوير تقنيه الـ SSL : Secure Socket Layer وأمنت هذه الطريقة قيام اتصال امن مشفر Encrypted ضمن تعقيدات متفاوتة فمنها الـ ٤٠ Bit ومنها ١٢٨ bit ،، فتم استخدام الـ SSL لتشفير وحماية قنوات الأتصال التي تنتقل عبرها الداتا مثل SMTP او الـ Database communications ،

وتم استخدام ما يعرف بـ SSL over HTTP في المواقع التجارية ومواقع الايميل فأصبحت تسمى HTTPS : Secure Hyper Text Transfer Protocol واستخدم بورت٤٤٣ بدلا من ٨٠ الخاص بـ HTTP ،وانتشر واشتهر بشكل كبير.

ثم ظهرت تقنيه مشابه له ولاستخدامه وهي الـ TLS : Transport Layer Security وهي تقنيه محسنه من الـ SSL ولكنهما يختلفان في طريقة أداء العملية ،، والطريقتان تحتاجان للشهادات الالكترونية Certificates أو بالأحرى Web-based Certificates .

كما وظهرت تقنيه أخرى داخل الشبكة نفسها وليس على شبكه عالميه كالانترنت ،وهي SMB Signing ،، الجميع يعلم أن الـ : SMB Server Message Block هي الـ packets إلى يتم إرسالها بين

السير فر والأجهزة في عملية المشاركة في الملفات وغيره Sharing ،،
وللحماية من طريقة سرقة المعلومات أثناء مرورها في الأسلاك Man In The Middle MITM وهذه ألطريقه تدعى SMB Signing ،، يتم بواسطتها إضافة الـ - Hash (وهي طريقة يتم من خلالها استخلاص رمز معين حسب حسابات رياضيه من الرسالة ، ومن الأمثلة عليه MD4 , MD5 , SHA-1) ويتم تشفير هذا ال - Hash وإضافته للرسالة وبذلك نحافظ على صحة الرسالة Message or Packet Integrity .

لكن ظهرت المشكلة الكبرى بكون جميع هذه الوسائل تعمل على الـ Application Layer في الـ OSI Model أي أن وظائفها محدده جدا ، لا تستطيع تشفير إلا ما بنيت لأجله ،، لذلك كان لا بد من ابتكار طريقة تمكننا من تشفير كل Packet تصدر من أي جهاز ،، فتم ابتكار تقنيه الـIP Security وهي تقنيه تعمل على الـIP Layer في الـ DOD Model أو الـ Network Layer في الـ OSI Model بمعنى انه يقوم بتشفير كل شيء يصدر عن الجهاز ويرسله على الشبكة Network بما أن الـ Network Layer هي الجهة التي من خلالها يمرر كل شيء للشبكة. IPSec تقنيه توفر الموثوقية والصحة والتشفير لكل شيء يمر من خلالها على مستوى الـIP Packet .

٦.١- فوائد IPsec في الحماية :

١. موثوقية البيانات Data authenticity :

أي أن البيانات المرسلة من هذا المستخدم هي منه وليست مزوره أو مدسوسة على الشبكة .

٢. صحة البيانات Data Integrity :

أي أن البيانات المرسلة لم يتم تعديلها على الطريق أثناء مرورها على الأسلاك .

٣. عدم إعادة الإرسال Anti-Replay :

وهذه الطريقة التي ستخدمها المخترقون حيث يقومون بسرقة الباسوورد وهي مشفره ويقومون بإعادة إرسالها في وقت أخر للسيرفر وهي مشفره وطبعا يفك السيرفر التشفير ويدخل اليوزر على أساس انه شخص أخر،، فإن الـ IPSec يقدم حلولا لمنع هذه العملية من الحدوث.

٤. حماية ضد الخداع Anti-Spoofing protection :

ويوفر أيضا الـ IPSec حماية ضد الخداع من قبل المستخدمين ، مثلا يمكن أن يحدد مدير الشبكة انه لا يسمح لغير المستخدمين على الـ 192.168.0.X subnet بينما لا يسمح لحاملي الهوية ١٩٢.١٦٨.١.x من دخول السيرفر ، فيمكن للمستخدم أن يغير ال IP Address خاص به ، لكن الـ IPSec يمنع ذلك .(وأيضا يمكنك

القياس على ذلك من خارج الشبكة الى داخلها) يكون لكل الحزمة Packet موقعه Digitally signed.

• ويمكن تخليص الأمور التالية الى :

الموثوقية (Authenticity):

موثوقية البيانات Data authenticity :أي أن البيانات المرسلة من هذا المستخدم هي منه وليست مزوره أو مدسوسة على الشبكة . ويتم ضمان ذلك باستخدام طريقة IPSec

السرية (Confidentiality):

حماية محتوى حزم المعلومات من الإفشاء إلا للجهات المرسلة إليها. وهذه خاصية من خاصيات طريقة IPSec

سلامة البيانات المنقولة (Data Integrity):

صحة البيانات Data Integrity : أي أن البيانات المرسلة لم يتم تعديلها على الطريق عند تنقلها من خلال الشبكة .

تخمة الشبكات (Saturation)

من المعروف أن من أخطر ما يهدد الشبكات هذه الأيام هي الهجمات التي تؤدي إلى تخمة الشبكة (Saturation) وذلك بحجب الخدمة التي قد تتعرض لها وفي كثير من الأحيان يصعب تفاديها إن تمت بصورة دقيقة ومركزة. منفذي هجمات حجب الخدمة الموزعة DDoS أو Distributed Denial of Service يحتاجون إلى عدد كبير من الأجهزة لكي ينفذوا هجماتهم فتراهم يبرمجون برمجيات تعمل على أتمتة

الهجوم و الاستيلاء على أجهزة الحاسب و من ثم الانتقال إلى الأجهزة المجاورة و غيرها بصورة تلقائية سريعةأو إذا كان جهاز الحاسب غير محمي بصورة كافية فانه سيقع ضمن قائمة الأجهزة التي تنتظر الأوامر من المهاجمين لتنفيذ الهجوم. في العادة فان الأجهزة المصابة لا يتم حذف الملفات منهاألكن يتم استعمالها جميعاً في وقت واحد في الهجوم على شبكة معينة أو موقع معين و تلك الأجهزة تسمى zombies.

٧ـ **التشفير** (Encryption) :

التشفير استخدم قديما في الحضارات القديمة لإخفاء المعلومات والمراسلات مثل الحضارة الفرعونية والدولة

الرومانية .ولكن التشفير كعلم مؤسس منظم يدين بولادته ونشأته للعلماء الرياضيين واللغويين العرب إبان العصر الذهبي للحضارة العربية ومن أشهرهم الفراهيدي والكندي، وقد ألف هؤلاء العلماء مفاهيم رياضية متقدمة من أهمها التوافيق والتباديل . وكذلك توظيف الكندي ومن تبعه مفاهيم الإحصاء والاحتمالات في كسر الشفرة ، وقد سبقت هذه الكتابات كتابات باسكال وفيرما بحوالي ثمانية قرون !!!وقد شاع في أيامنا استخدام مصطلح" التشفير"ليدل على إخفاء المعلومات .ولكن كلمة" التشفير"وافدة من اللغات

وهذه بدورها جاءت أصلا من اللغة العربية ولكن بمعنى آخر لكلمة "الصفر ".فكما هو معلوم أن العرب قد (Cipher) الأوربية تبنوا

مفهوم الصفر والخانات العشرية واستخدموه في الحساب، وهو ما لم يكن الأوربيون يعرفونه في القرون الوسطى ، ولأن مفهوم الصفر الجديد كان في "Cipher". وكان مفهوم الصفر جديدا وغريبا لدرجة أنهم أخذوه بنفس الاسم فأسموه للدلالة على الأشياء المبهمة وغير الواضحة "Cipher" .منتهى التعقيد والغموض فقد صاروا يستخدمون كلمة في جميع اللغات الأوربية تقريبا لتعني إخفاء المعلومات وقمنا – نحن العرب بعد "Cipher" ومن هنا تطور استخدام كلمة ستة قرون بإعادة بضاعتنا الأصلية ولكن بمعنى مختلف فنحتنا كلمة غريبة على اللغة العربية هي" التشفير."

لذا فإن الفيروس هي عملية الحفاظ على سرية المعلومات (الثابت منها و المتحرك) باستخدام برامج لها القدرة على تحويل وترجمة تلك المعلومات الى رموز بحيث إذا ما تم الوصول إليها من قبل أشخاص غير مخول لهم بذلك لا يستطيعون فهم أي شيء لأن ما يظهر لهم هو خليط من الرموز والأرقام و الحروف الغير مفهومة.

ولقد شهدت أسواق هذه البرامج انتعاشا مذهلا بعد أن سمحت السلطات الأمريكية للشركات التجارية المتخصصة ببيع هذه التقنية للجمهور و عامة الناس بعدما كانت محصورة للاستخدامات العسكرية والحكومية لسنوات طويلة ولقد اتخذت الحكومة الأمريكية هذا القرار في سبيل دعم الجانب الأمني لمجال التجارة الإلكترونية علما بأنها وحتى

وقت قريب جدا لم تسمح بتصدير هذه التكنولوجيا إلى خارج الولايات المتحدة، خاصة للتي تزيد قوة تشفيرها عن ٥٦ بت.

٧.١- فكرة عامة و مبسطة عن التشفير:

على اختلاف أنواع و أشكال البرامج المتخصصة في هذا المجال إلا أنها جميعا تتشارك في القاعدة أو الأساس وهي مبنية على مفهوم بسيط جدا وهو أن كل رقم أو معلومة مشفرة تحتاج لفكها و إعادتها الى وضعها الأصلي إلى ثلاث عناصر مجتمعة مع بعضها البعض و لنفرض انها (س ، ص ، ع) أما في حالة معرفة قيمة واحدة فقط من هذه العناصر و بقاء الاثنتين الباقيتين مجهولتين فإنك سوف تجد نفسك في دوامة الاحتمالات والتخمين للوصول إلى القيم الصحيحة لهذين العنصرين المجهولين اللازمين لإكمال الحلقة و فك الشفرة وعلى هذا الأساس علينا التعرف على ثلاث مصطلحات لفهم هذه التكنولوجيا : المفتاح العام ، المفتاح الخاص ، و الرقم الأساس حيث أن أي معلومة يتم تشفيرها لا يمكن الاطلاع عليها صحيحة وكاملة إلا بوجود هذه المفاتيح الثلاثة مجتمعة

٧.١.١- ويتم تطبيق هذا المبدأ في مجال التشفير كالتالى :

يتم إصدار رقم الأساس عن طريق البرنامج المتخصص أو احد الهيئات المستقلة و المتخصصة في إصدار هذه الأرقام وهو مايعرف بـ

Certificate Authority

بحيث يكون لكل مستخدم رقم أساس وهو (ع) و يتم تقسيم هذا

الرقم إلى مجموعتين (س) و هو ما يعرف بالمفتاح العام و (ص) هو ما يعرف بالمفتاح الخاص ، بحيث إذا قمنا بعملية ضرب س في ص يكون الناتج هو (ع) الرقم الأساس وهو الرقم اللازم لإعادة الملفات و المعلومات إلى وضعها الأصلي قبل التشفير وطبعا هذا الرقم محمي ومشفر بقوة ولا يمكن الوصول إليه.

٧.١.١.١- **المفتاح العام** : (Public Key)

هو الرقم الذي يتم تداوله و نشره بين بقية المستخدمين لتشفير أي معلومات أو رسالة الكترونية مخصصة لك و يعتبر رقمك العام أساس عملية التشفير و لا يستطيع أحد فك رموز تلك المعلومة غيرك أنت لأنها تحتاج إلى الرقم السري و ليكن هو المفتاح الخاص بك لإكمال العملية الحسابية والوصول إلى الرقم الأساس وبالتالي فتح الملفات مرة أخرى.

٧.١.١.٢- **المفتاح الخاص** : (Private Key)

هو النصف الآخر المكمل للمفتاح العام للوصول الى الرقم الأساس واعادة المعلومات المشفرة الى وضعها الطبيعي قبل التشفير ، و هذا المفتاح هو الذي يميز كل شخص عن غيره من المستخدمين ويكون بمثابة هوية الكترونية تمكن صاحبها من فك أي معلومة مشفرة مرسله اليه على أساس رقمه العام ولذلك يجب عليك الاحتفاظ بالمفتاح الخاص سرا وهذا ما يعرف بـ Private Key

و بهذه الطريقة لا يستطيع أحد فك الشفرات وقراءة المعلومات المحمية بهذه الطريقة دون اكتمال الحلقة و التي لا تتم إلا بمعرفة القيمة الصحيحة للمفتاح العام و المفتاح الخاص

٧.٢- أنواع تكنولوجيا التشفير:

هنالك نوعين من التكنولوجيا المستخدمة في التشفير وهي التشفير المتناظر والتشفير الغير متناظر Symmetric Algorithms and ASymmetric Algorithms

و الفرق بينهم بسيط جدا ولكنه مهم جدا في مستوى ودرجة الأمن حيث أن التشفير المتناظر يتم بتشفير الرسالة أو المعلومات باستخدام الرقم العام وكذلك في نفس الوقت يتم فك الشفرة و ترجمة المعلومات إلى وضعها الأصلي باستخدام نفس الرقم العام. ولذلك لو حصل و أن شخص آخر يعرف هذا الرقم أو حصل عليه من الدليل العام فإنه قادر على فك الشفرة و قراءة تلك الرسالة أو المعلومة ، أما إذا ما تم تشفير المعلومات بأسلوب (الغير متناظر) فإن المعلومات يتم تشفيرها بالرقم العام ولكن لا يمكن فك الشفرة و الوصول إلى تلك المعلومات الا بالمفتاح الخاص لصاحب ذلك المفتاح العام الذي تم على أساسه عملية التشفير

و للتسهيل ، تخيل بأنك تقوم بالاتصال هاتفيا بأحد أصدقائك وعندما تدخل رقم هاتفه (الرقم العام) ويبدأ هاتفه بالرنين ولكن ذلك الصديق

لا يرد على مكالمتك فيرد عليك جهاز إجابة و تترك له رسالة صوتية في ذلك الجهاز . و الآن لنتخيل بأنك قمت بحماية (تشفير) تلك الرسالة برقم سري و لا يستطيع أحد الاستماع إلى تلك الرسالة إلا بإدخال ذلك الرقم السري. فإن كان صديقك هذا قد اتفق معك على اختيار الرقم السري هو نفس رقم هاتفك العام فهذا ما يسمى بطريقة التشفير المتناظر لأن المفتاح العام = الرقم السري أما لو قام ذلك الصديق ببرمجة التشفير لطلب الرقم السري الخاص بك (رقم آخر لا يعرفه أحد غيرك) فهذا ما يعرف بالتشفير الغير متناظر لأن المفتاح العام لا يساوي الرقم السري.

١.٢.٧- أشهر طرق التشفير المتناظر :

Blowfish, Digital Encryption Standard (DES), Tiny Encryption Algorithm(TEA), Triple DES, and International Data Encryption.

٢.٢.٧- أشهر طرق التشفير الغير متناظر

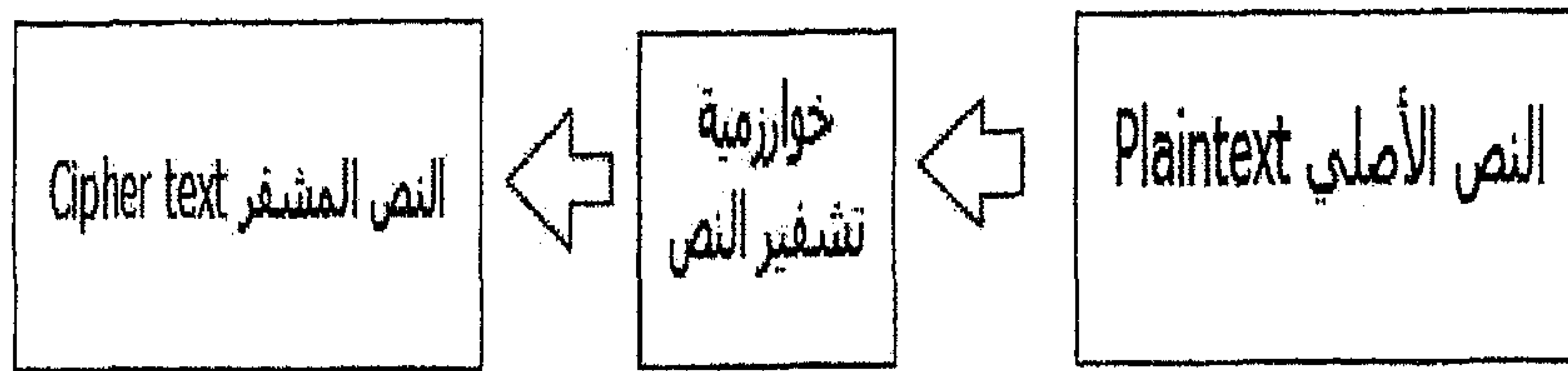
Pretty Good Privacy(PGP) and Reivest,shamir&Aselman(RSA)

٣.٧- قوة التشفير:

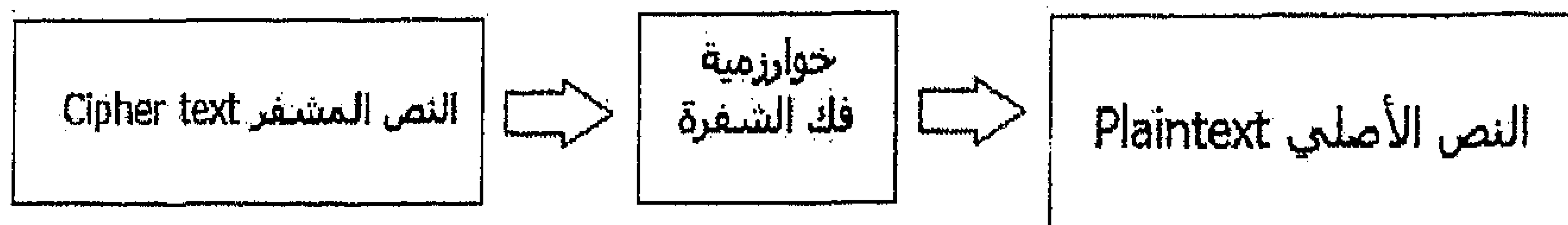
تعتمد على عدد الخانات المكونة لكل رقم و تقاس ب البت فمثلا إذا كان الرقم مكون من ٤٠ خانة فإن القوة ستكون ٤٠ بت إذا كان الرقم

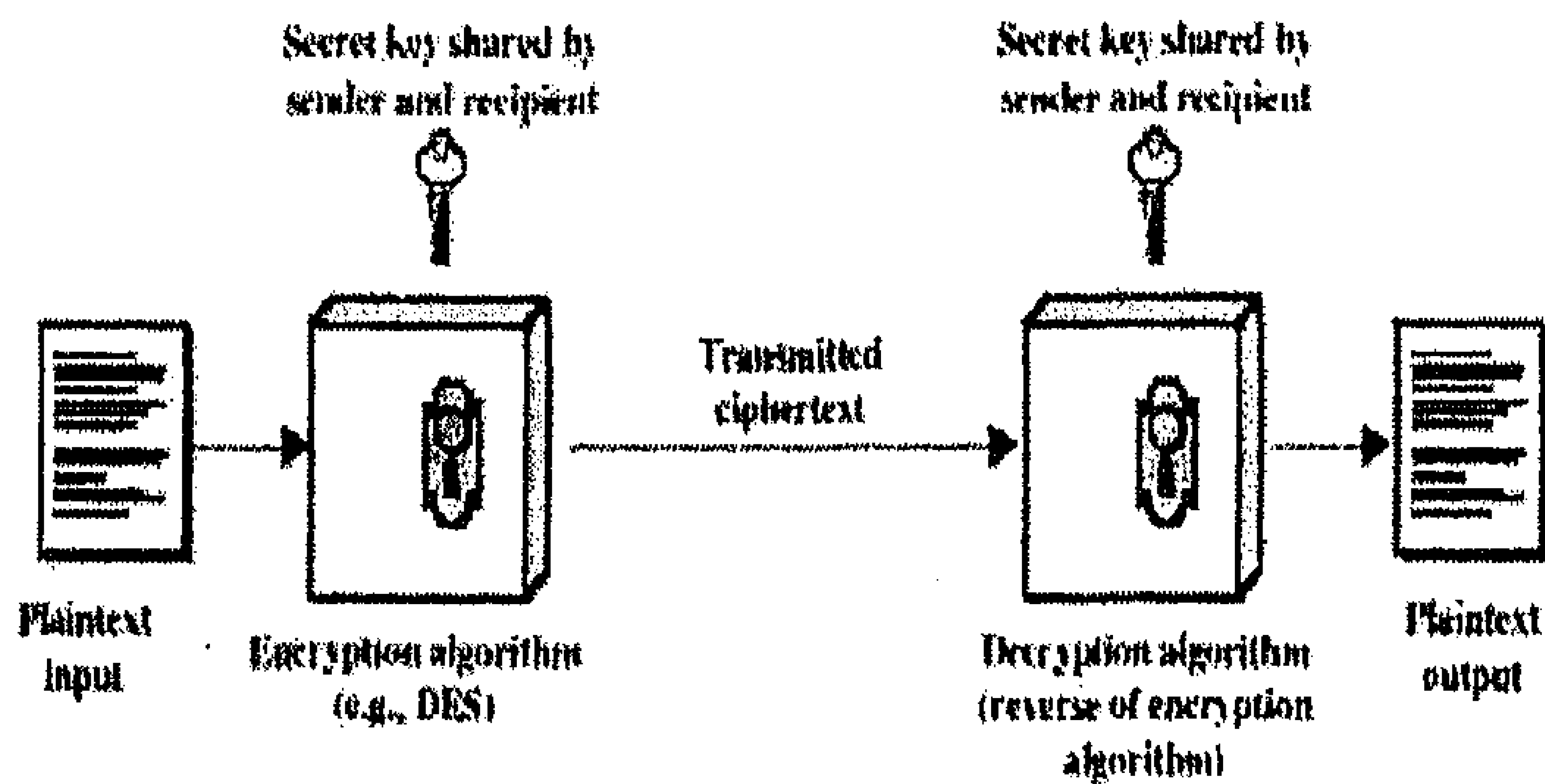
عبارة عن 56 خانة تكون قوة التشفير ٥٦ بت وهكذا. علما بأن التكنولوجيا المتوفرة في هذا المجال يمكن أن توفر قوة تشفير تصل إلى أكثر من ٣٠٠٠ بت ولكن لم تسمح الحكومة الأمريكية حتى الآن بتداول قوة تشفير أكثر من ١٢٨ بت لأنه كاف جدا لحماية التجارة الإلكترونية و جدير بالذكر أن الوقت اللازم ليتمكن أحد لصوص الإنترنت لفك شفرة بقوة 56 بت هو ٢٢ ساعة و خمسة عشر دقيقة ، أما الوقت اللازم لفك شفرة بقوة ١٢٨ بت باستخدام التكنولوجيا الحالية لفك الشفرات فهو ٢ ترليون سنة!! لأن اللص في حالة ٥٦ بت بحاجة لتجربة ٧٢ كوادرليون من الاحتمالات (يعني رقم و أمامه ١٥ صفر) أما في قوة 128 فإن الاحتمالات المطلوبة للتجربة تصل الى عدد فلكي وهو ٣٤٠ انديسليون (يعني رقم وأمامه ٣٦ صفر) ولذلك لم نسمع أبدا بأن معلومة تم تشفيرها بهذه القوة قد تم فكها من قبل هؤلاء اللصوص المحترفين و نحن لا نعتقد بأن أحد يمكنه فعل ذلك على الأقل في المستقبل القريب أو المنظور ولذلك تسوق على شبكة الإنترنت وأنت مطمئن البال بشرط التأكد من قوة التشفير المستخدمة من قبل الموقع الذي تود الشراء منه و كذلك التأكد من قوة التشفير في متصفحك.

إذاً التشفير : هو تحويل المعلومات المهمه أو التي لا تريد أن يطلع عليها أحد إلى نص مخفي(أي لا يمكن فهمه)



وعملية فك التشفير كالتالي:





وكمثال بسيط على ذلك نأخذ على سبيل المثال كلمة Arab : الخطوات أو الخوارزمية لتشفير تلك الكلمة

نجعل كل حرف يساوي الحرف الذي تليه أي أن:

A = B
R = S
A = B
B = C

وفي هذا المثال النص الأصلي plaintext هو Arab والنص المشفر هو BSBC وبذلك قد أخفينا النص الأصلي وعندما تصل إلى الطرف الثاني فإنه يقوم بعكس التشفير أي أننا:

نجعل كل حرف يساوي الحرف السابق ، وبذلك قد حصلنا على النص الأصلي.

إن وجود برنامج حماية من قراصنة الكمبيوتر بجهازك، لا يعني عدم قدرتهم على اختراقه. إذا اعتقدت أن وجود عدة برامج حماية بجهازك ، وتعمل في آن واحد سوف يحمى جهازك و يزيد من فعالية الحماية فهذا خاطئ ،لأن ذلك يضعف من إمكانية الحماية على الجهاز .

إن هدف ٨٠ في المئة من القراصنة هو الحصول على اشتراكك و رقمك السري وبريدك الإلكتروني ورقمه السري ، لأهداف كثيرة وخطيرة جدا، منها الابتزاز والتخريب الذي يتم بسهولة لو تم الاختراق .

أما الـ ٢٠ في المئة الباقون، فهدفهم الرئيسي هو التجسس والإطلاع على محتويات جهازك ومعلوماتك الشخصية وصورك الخاصة، وسحب ملفات أو برامج، أو مسحها كلياً من جهازك وهذه الفئة تندرج تحت مسمى الهواة .

إلى هنا نأتي لعرض بعض الطرق لتفادي تلك الأمور المؤدية إلى إتلاف أجهزة الحاسوب ومعلوماتها :

٨ـ طرق حماية جهاز الحاسوب :

لا شك أن المعلومات تختلف من منشأة إلى منشأة وعلى حسب أهمية المعلومات فأن المنشأة تتخذ الإجراء المناسب وقد يكون تدخل بعد حدوث الخطر) انفعالي أو عاطفي Proactive Model (، وقد يكون التدخل قبل حدوث الخطر ويسمى Reactive Model. .

ويسمى

Attacks أو الهجوم Threats وهنا بعض أمثلة الإجراءات المضادة للتهديد:

- Firewalls.وضع جدران نارية.
- Anti-virus software.برامج مكافحة الفيروسات.
- Access Control.التحكم بالدخول.
- الحماية بكلمات المرور.
- بروتوكولات الحماية.
- نماذج الأمان.
- Two-factor authentication systems.مضاعفة أنظمة التحقق من المستخدم.
- Well-trained employees.التدريب الجيد للموظفين.
- التدريب المتقن للمستخدمين على التعامل مع إجراءات الأمن.

• التأكد من أمن المعدات و صعوبة الوصول إليها من قبل غير المخولين.

• حماية الأسلاك النحاسية و إخفاءها عن الأعين لأنها قد تكون عرضة للتجسس.

• تشفير البيانات عند الحاجة أما مقاييس التشفير فتضعها وكالة الأمن الوطني الأمريكية National Security Agency (NSA).

• تزويد المستخدمين بأجهزة لا تحتوي على محركات أقراص مرنة أو مضغوطة أو حتى أقراص صلبة ، و تتصل هذه الأجهزة بالمزودات باستخدام رقاقة إقلاع ROM Boot Chip و عند تشغيل هذه الأجهزة يقوم المزود بتحميل برنامج الإقلاع في ذاكرة RAM للجهاز ليبدأ بالعمل.

•استخدام برامج لتسجيل جميع العمليات التي يتم إجراؤها على الشبكة لمراجعتها عند الضرورة.

• اعمل نسخ احتياطي Backup بشكل معتاد للبيانات: احتفظ بنسخة من سيدي للملفات المهمة .استخدم برنامج خيارات أو أدوات الـ. backup وأحفظ هذا الديسك بعيدا عن الجهاز لحين حاجته.

• اعمل قرص التشغيل boot disk لكمبيوترك في حالة تعرضه لأخطار جسيمة:

للمساعدة في التعافي من فشل القرص الصلب أو اختراق أمني . اختر

قرص التشغيل (فلوبي ديسك (disk Floppy) الذي سيساعدك عند استعادة الجهاز في حال حدوث شيء.

8.1- بعض الطرق التقنية والمهارة لحماية الأجهزة والمعلومات في الشبكة:

٨.١.١- يجب التأكد من عدم وجود تروجان بجهازك، والتروجان هو خادم يسمح للمخترق بالتحكم الكامل في جهازك، ويتم زرعه بجهازك عن طريق المخترق و ذلك بإرساله إليك عن طريق بريدك الإلكتروني مثلا أو عن طريق برامج الدردشة الفورية مثل ICQ أو عن طريق قرص مرن، أو تقوم أنت بزرعه في جهازك عن طريق الخطأ بسبب عبثك في برامج الاختراق · فتقوم بفك التروجان في جهازك، بدلا من أن ترسله إلى الجهاز المراد اختراقه ، لذلك أنصحك عدم تحميل هذه البرامج نهائياً ، ولكي نتأكد ما إذا كان بجهازك تروجان أم لا، هناك عدة طرق مثل البحث في ملف السجل Registry الخاص بالوندوز، ولأهمية الريجستيري ولتفادى حذفك الملفات عن طريق الخطأ سوف نبحث عن التروجان بطريقة آمنة و ذلك باستخدام برامج باحثة · الذي يعد أفضل برنامجCleaner The فإذا لم يكن متوفرا لديك، قم بتحميله فوراً وهو برنامج.

٨.١.٢- قم بتحديث البرنامج المكافح للفيروسات لديك دائماً ، فبرنامج الفيروسات يقوم أحياناً بكشف التروجان عند فتحه عن طريق

تحديث البرنامج الموجود على جهازك لأن عمل UPDATE باستمرار من على الإنترنت · فيكون قد تم وضع آخر إصدار لهذه البرامج المكافحة للفيروس والتروجان من على الموقع الخاص ببرنامج المكافحة ومدك أيضاً بأحداث أسماء للفيروسات والتروجان الذي أنصحك دائماً بعمل UPDATE للبرنامج الخاص بك باستمرار · وأيضاً معرفة أحدث البرنامج المكافحة للفيروسات والتروجان من خلال شبكة الإنترنت

٨.١.٣- استقبل الملفات أو البرامج أو الصور من أشخاص تثق بهم فقط ، وإن لم تفعل ذلك، فعلى الأقل لا تقم بفتحها إلا بعد انقطاعك عن الاتصال ، وبعد فتحها جميعاً قم بعملية بحث عن التروجان بواسطة برنامج Cleaner على قرصك الصلب لتتأكد من خلوه من التروجان، فالتروجان له خاصية الذوبان في النظام ، علماً بأن حجمه يتراوح من ٥٠ إلى ١٥٠ كيلو بايت حسب نوعيته و إصداره · (قد تستقبل صورة أو ملف و يكون التروجان مزروعا بداخلها لذلك احذر).

٨.١.٤- احذر الملفات التي تأتيك عن طريق البريد الإلكتروني، فإذا كان الملف المرسل إليك من شخص لا تثق به و من نوع dll أو exe فلا تستقبله أبداً

٨.١.٥- يفضل أن يكون رقمك السري مكونا من حروف وأرقام، ويكون أكثر من ٨ خانات ، كما يفضل تغييره على الأقل كل شهر · أنت

الآن في أمان من الهاكرز إن شاء الله . ثانياً : قم بعمل بحث عن التروجان بالضغط على زر بحث سكان Scan و بعد الانتهاء من البحث على قرصك الصلب، سيخبرك برنامج إن كان يوجد لديك تروجان مزروع بجهازك، وسيعطيك خيار حذفه أو عدمه ، طبعاً اضغط على الموافقة لحذفه · إذا انتهى البحث و ظهرت نافذة صغيرة مكتوب بها scan complete فهذا معناه أن جهازك خال و نظيف من التروجان ·

٦.١.٨- الحماية أثناء استخدام البريد الإلكتروني وذلك بإتباع الطرق التالية :

- استخدام برامج مضادة للفيروسات و برامج حماية و تشفير متخصص.
- استخدام كلمات عبور سهلة التذكر ولكن صعبة التخمين كأن تكون مكونة من حروف و أرقام أو خليط من الأحرف الكبيرة والصغيرة.
- غلق المتصفح حال ابتعادك عن الجهاز لتعطيل خاصية الرجوع للخلف في المتصفح .
- عدم استخدام خاصية تذكر اسم المستخدم وكلمة العبور.
- عدم استخدام خاصية الإكمال الآلي للاسم و فراغات النماذج في المتصفح .
- عدم استخدام خاصية تذكر الصفحات التي تقوم بزيارتها لفترات

طويلة و تقليل هذه المدة على قدر المستطاع.

- عدم فتح الملفات المرفقة إذا كانت من احد الأنواع المذكورة في بداية هذه المقالة .

- عدم تحويل الرسائل المشبوهة إلى أصدقائك و معارفك .

- تعديل خاصية الأمن في المتصفح الخاص بك إلى المستوى المتوسط أو الأعلى مع تعطيل خاصية الجافا سكريبت و تعديل مستوى الأمن في خاصية الأكتف إكس .

- عند الانتهاء من قراءة الرسائل عليك بالخروج بطريقة صحيحة (Sign out)من الموقع أو البرنامج لأن هنالك بعض برامج البريد أو المواقع تتذكرك لمدة تصل إلى ٨ ساعات و ترحب بك مباشرة حال دخول أي شخص آخر للموقع ذاته.

- لا تفتح الملفات المدمجة مع البريد الالكتروني المجهولة: قبل فتح أي ملفات مدمجة مع الإيميل. يجب أن تتأكد من المصدر لهذا الملف المرفق. ولكن أيضا لا يكفي بأن تفتح هذا الملف المرفق بمجرد أنك عرفت مصدره . لأنه قد يأتيك فايروس مثل الميليسا حيث كان يرسل نفسه من إيميلات إلى إيميلات أخرى تكون معروفة للأول (بسبب تسجيله في قائمة Notebook) وهكذا أخذ ينتشر بهذه الطريقة .وغالبا ما تدس هذه البرامج والكودات الخبيثة في برامج مسلية ومغرية. إذا كان لابد منك فتح الملفات المرفقة مع الإيميل بدون أن تعرف المصدر.

٨.١.٧- لا تقبل كوكيز :cookies فبعضها غير مأمون؛ إذ تقوم بتتبع عاداتك في الإبحار عبر الويب وتقدم تقريرا عما تتصفحه؛ فإذا أردت السماح ببعضها؛ فهناك بعض البرامج التي تقوم لك بتلك المهمة مثل Cookie Palو Cookie Crusher. امنع الكوكيز كلما استطعت وتجنب زيارة المواقع المحتوي علي الاكواد الشريرة او حتي وكن حذرا في التعامل مع ActiveX المدمجة في صفحات الويب.

٨.١.٨- لا تتحدث بدون حماية:

قد تظن أنك بمأمن عندما تتحدث مع من تعلم، ولكن الـ spammersوالمواقع تستخدم برامج تلتقط عناوين البرد الإلكترونية، حتى إذا لم تمدها أنت بها؛ لذا لا تشغل برامج التحادث الفوري instant messaging في خلفية جهازك، بمعنى أغلقها ما دمت لا تتحادث، وقد اعتاد البعض ما دام متصلا بالإنترنت أن يشغلها تاركا الفرصة لأصحابه أن يعرفوا أنه online ليقوموا بالاتصال به.

٨.١.٩- لا تشغل برامج مجهولة الأصل:

لا تشغل أبدا أي برامج إلا إذا عرفت مبرمجه وكنت تثق به سواء كان شخصا أو شركة. أيضا لا ترسل برامج مجهولة المصدر إلى زملائك وأصدقائك لأنها قد تحتوي على أكواد أو ملفات ضارة.

٨.١.١٠- حاول إطفاء جهازك الشخصي او فصله من الشبكة في حين عدم استعماله:

أطفئ الجهاز أو افصله من الشبكة اذا لم يمكن قيد الاستعمال. المخترق لا يمكنه اختراق جهازك إذا كان مغلق أو في حالة عدم اتصاله بالشبكة..

٨.١.١١- التأكد من الهوية :

يعنى التأكد من الهوية بكيفية اختبار المستخدمين فيما إذا أنهم فعلا المستخدمين الحقيقيين|إن طرق التحقق من الهوية تتراوح من وجود رقم معرف و كلمة سر خاصة بكل مستخدم إلى طرق التأكد التي تعتمد على معدات هاردويرية مثل التأكد عن طريق بطاقات ممغنطة أو التأكد من البصمة و حدقة العين و طبعا يتراوح استخدام هذه التقنيات حسب الأهمية و الحاجة.

٨.١.١٢- المراقبة و المراجعة :

ما إن تقوم بوضع سياستك الأمنية لشبكتك و تنفذها عليك بعد فترة التأكد من أن المكونات و الموظفون يطبقون و يلتزمون هذه السياسة و يتم ذلك بمراقبة تطبيق هذه السياسةأ تفيد السياسة في التعرف على المشاكل و التنبؤ بها قبل حدوثها و يجب مراجعة السياسة باستمرار للتأكد من استمرار فعاليتها.

٨.١.١٣- **خطة طوارئ:**

يجب أن تحتوي سياستك على قسم يشرح الإجراءات الواجب اتخاذها في حال حدوث كارثة و بالتالي عليك تحديد كيفية و توقيت استرجاع البيانات عند حدوث هجوم يؤدي لضررها و تحديد كيفية صد هجوم و كيفية حفظ النسخ الاحتياطية و مكانها و المسئولون عليها.

وفي ما يلي عشرة إرشادات للبدء في إتباع إستراتيجية تأمين ووقاية ناجحة لوقاية شبكة الأجهزة من أخطار الفيروسات ولصوص المعلومات:

١ ـ لا بد من رسم سياسة تأمين ووقاية شاملة. في هذا السياق يقول أليكساندر دول، وهو المدير التنفيذي لشركة «بي جي بي» لإنتاج برامج تأمين ووقاية شبكات الكومبيوتر في بالو التو في كاليفورنيا، أن وسائل الأمن والحماية لا يجب أن تقتصر بالضرورة على ما تعنيه عملية التأمين والوقاية من نقطة البداية وانتهاء بقواعد المعلومات، إنما يجب أن تحتوي أيضا على المسؤوليات إزاء التحديثات التي تطرأ على تقنيات التأمين والوقاية والتصريح بدخول الشبكات التي تضم أجهزة لاسلكية وحساب الاشتراك، كما يجب أن تغطي سياسة الوقاية والتأمين كيفية تعامل المؤسسة مع قضايا أمن شبكتها.

٢ ـ يجب تشفير أي وثائق مهمة بالشبكة، وهذه تشمل معلومات الزبائن والمعلومات الخاصة بالشركة أو أي أشياء أخرى يمكن أن تلحق ضررا

بالشركة سواء كان ذلك بصورة مباشرة أو غير مباشرة، إذا وقعت هذه المعلومات في أيد أخرى غير مأمونة. بمعنى آخر، إذا فقد مسؤول جهاز كومبيوتر حضني نتيجة السرقة أو لأي سبب آخر، فإن المعلومات الخاصة بالزبائن أو أي معلومات خاصة أخرى، لا تكون ذات قيمة بالنسبة للص او الشخص الذي يعثر على الجهاز المفقود. لا ينبغي أيضا تشفير كل المعلومات الموجودة على الجهاز، على سبيل المثال لا حاجة إلى تشفير قائمة الطعام التي تقدمها كافتيريا الشركة.

٣ ـ من الأفضل استخدام تقنيات تأمين وحماية شبكات الكومبيوتر الخاصة بالمؤسسات والشركات في الاتصال بالأجهزة، إذ أن ذلك يسمح بالدخول إلى الموقع الخاص بالشركة لكنه لا يسمح بالدخول الى البرامج المتاحة فقط للأشخاص المصرح لهم.

٤ ـ من المستحسن الحد من الاطلاع على الملفات وتحديد الأجزاء المراد الاطلاع عليها باستمرار بواسطة العاملين في الشركة، فمندوبو المبيعات، على سبيل المثال، يحتاجون الى الاطلاع على المعلومات الخاصة بالزبائن، مثل الاسم والعنوان والمشتريات السابقة من الشركة، إلا انهم لا يحتاجون إلى الاطلاع على تفاصيل ومعلومات بطاقات الائتمان الخاصة بزبائن الشركة، لأن ذلك من اختصاص قسم الحسابات. لذا، فإن مندوبي المبيعات ليسوا في حاجة إلى الإطلاع على الملفات وقواعد المعلومات الخاصة بمثل هذه التفاصيل. كما أن المهندسين الفنيين

العاملين لشبكة الكومبيوتر، ربما يحتاجون إلى معلومات فنية ذات صلة بعملهم في الشبكة، لكنهم ليسوا بالتأكيد في حاجة إلى التفاصيل والمعلومات الخاصة بإدارة العلاقات مع زبائن الشركة.

٥ ـ استخدم تكنولوجيا المسح للتعرف على الأجهزة السلكية واللاسلكية الداخلة في الشبكة لمعرفة ما إذا كان مصرحا بذلك، كما من الأفضل أيضا متابعة الإضافات الجديدة لبرامج ويندوز ورصد الفيروسات، علما بأن الأخطار يمكن أن تأتي من أجهزة الكومبيوتر الحضني غير المحمية التي من المحتمل آن تكون قد تعرضت لفيروسات خلال استخدامه خارج الشبكة، ما يعني احتمال نقلها لهذه الفيروسات عند استخدامها في الدخول إلى الشبكة الخاصة بالشركة أو المؤسسة، وهذا في حد ذاته يعتبر أكثر خطورة من التهديد الذي يشكله المتسللون.

٦ ـ يقول خبراء متخصصون في تأمين وحماية الشبكات انه من الأفضل عدم السماح للأشخاص الآخرين باستخدام أجهزة الكومبيوتر الحضني المستخدمة في الشبكة، وذلك بتزويدها بأرقام سرية أو كلمات مرور وبرمجتها على أساس أن تغلق تلقائيا بعد فترة محددة في حال عدم استخدامها.

٧ ـ من المهم تزويد الشبكة بتقنية حماية الشبكات WPA، وهي تقنيات حماية تتطلب من الشخص استخدام رمز أو شفرة محددة للدخول إلى

الشبكة مثل التقنية المستخدمة في الشبكات التي تحتوي على أجهزة سلكية ولاسلكية على حد سواء.

٨ ـ لا بد من إجراء اختبار للتأكيد من عمل تقنيات التأمين والوقاية على النحو المتوقع مثل السماح لأشخاص موثوق فيهم بمحاولة التسلل إلى الشبكة باستخدام كومبيوتر حضني لاسلكي وللتأكد أيضا من سهولة دخول الشبكة للأشخاص المصرح لهم بذلك.

٩ ـ من الأفضل استخدام أكثر من وسيلة للدخول إلى الشبكة المحلية سعيا لحماية أفضل للأجهزة والشبكة بكاملها. بدلا عن الاعتماد على رقم سري فقط للدخول إلى الشبكة، يمكن استخدام رقم سري وكلمة مرور أيضا.

١٠ ـ مراقبة النتائج ومراجعتها خطوة مهمة في جانب تأمين وحماية الأجهزة والشبكات على حد سواء، وفهم المسائل المتعلقة بتأمين الأجهزة والشبكات الخاصة ووقايتها من التسلل والفيروسات عملية مستمرة وتحتاج إلى متابعة متواصلة للجديد في هذا المجال، وهذا أمر يجب أن يدركه المهندسون الفنيون للكومبيوتر والموظفون على حد سواء.

الوحـــدة الثـانيـــة

التعرف على إعداد النسخ الاحتياطي
من نظم التشغيل والتهيئة للأجهزة

المقدمة:

يساعد النسخ الاحتياطي للملفات على حمايتها من التعرض للفقدان أو التغيير بشكل دائم في حالة حدوث حذف مفاجئ، أو هجوم أحد الفيروسات المتنقلة أو الفيروسات، أو تعرض أحد البرامج أو الأجهزة لعطل. إذا حدث أي شيء من هذه الأشياء وقد تم نسخ الملفات احتياطياً، يمكنك بسهولة استعادة تلك الملفات. لنسخ الملفات احتياطيًا، راجع نسخ الملفات احتياطياً.

فالنسخة الاحتياطية للملف هي نسخة من أحد الملفات يتم تخزينها في أحد المواقع المنفصلة عن موقع الملف الأصلي. يمكنك امتلاك عدة نسخ احتياطية لأحد الملفات إذا أردت تعقب التغييرات التي تمت على هذا الملف.

يتم إجراء عملية النسخ الاحتياطي لآخر إصدار تم حفظه لكل ملف، ولذلك تحتاج أي ملفات تقوم بتغييرها أثناء النسخ الاحتياطي إلى أن يتم نسخها احتياطياً في المرة التالية. يمكنك جدولة عمليات النسخ الاحتياطي التلقائي كي تحدث أثناء الليل أو في وقت لا تستخدم الملفات فيه. لا يزال بإمكانك إجراء أشياء مثل قراءة رسائل البريد-الإلكتروني أو استخدام إنترنت أثناء تنفيذ إحدى عمليات النسخ الاحتياطي.

١ - أنواع النسخ الاحتياطية :

ينبغي أن تنسخ الملفات الشخصية والبرامج وإعدادات النظام احتياطيًا. ينبغي أن تقوم بإنشاء نقاط الاستعادة حتى يمكنك استعادة الكمبيوتر إلى إحدى الحالات السابقة عند الضرورة. يصف الجدول التالي كل نقطة من هذه النقاط.

لإجراء النسخ الاحتياطي استخدم وقت إجراء النسخ الملفات الشخصية مثل الصور والموسيقى والمستندات معالج النسخ الاحتياطي للملفات و ينبغي أن تنسخ الملفات، التي تقوم بإنشائها وتعديلها، احتياطيًا بشكل منتظم. إنها لفكرة جيدة أن تنسخ الملفات احتياطيًا قبل أي تغييرات على النظام، مثل إضافة أجهزة جديدة، أو تحديث برامج التشغيلأ أو تحرير السجل، أو إجراء تغييرات على Windows, مثل تثبيت إحدى حزم الخدمة. للحصول على مزيد من المعلومات حول نسخ الملفات احتياطياً، راجع نسخ الملفات احتياطياً.

معالج 'النسخ الاحتياطي للملفات' مضمن في:

Windows Vista Home Basic و ،Windows Vista Home Premium و ،Windows Vista Business ، Windows Vista Enterprise و ،Windows Vista Ultimate

٢ - طرق تخزين النسخ الاحتياطية :

يمكنك نسخ الملفات احتياطيًا على أي نوع من أنواع التخزين التالية:

١.٢ - الأقراص الثابتة (الداخلية والخارجية).

٢.٢ - الأقراص الأخرى القابلة للنقل.

٣.٢ - أقراص DVD والأقراص المضغوطة القابلة للكتابة.

٤.٢ - مواقع الشبكة.

٣- المحافظة على النسخ الاحتياطية في أحد المواقع الآمنة :

قم دومًا بالمحافظة على الوسائط والتخزين القابل للنقل للنسخ الاحتياطية (مثل الأقراص الثابتة الخارجية، أو أقراص DVD، أو الأقراص المضغوطة) في أحد المواقع الآمنة لمنع الأشخاص غير المخولين من الوصول إلى الملفات.

٤ - أجهزة التخزين:

الأقراص الثابتة الداخلية. يمكنك تثبيت (أو جعل شخص آخر يقوم بالتثبيت) قرص ثابت خارجي ثان في الكمبيوتر واستخدامه لنسخ الملفات احتياطيًا. الأقراص الثابتة رخيصة نسبيًا ولا تتأثر إذا كان لديك مشكلة في نظام التشغيل.

ملاحظة

لا تنسخ الملفات على الإطلاق عل أحد المواقع على نفس القرص الثابت الذي تم تثبيتWindows عليه، نظرًا لأنه إذا تعرض الكمبيوتر إلى

أحد الفيروسات أو تعرض أحد البرامج فيه للتلف، قد يلزم إعادة تهيئة القرص أو إعادة تثبيت Windows للخروج من هذه المشكلة

٤.١ - الأقراص الثابتة الخارجية:

في حالة وجود منفذ USB في الكمبيوتر أيمكنك إرفاق أحد الأقراص الثابتة الخارجية له ثم نسخ الملفات احتياطياً إلي القرص الخارجي. تأكد أنك ستقوم بشراء أحد الأقراص الثابتة الخارجية التي لديها مساحة كبيرة تسع الملفات المنسوخة احتياطياً (٢٠٠ غيغا بايت يعتبر اختيار جيد). للحصول على الحماية القصوى، عليك الاحتفاظ بالقرص الثابت الخارجي في أحد المواقع المضادة للحريق المنفصلة عن الكمبيوتر.

٤.٢ - الأقراص القابل للكتابة :

يمكنك أيضاً حفظ الملفات إلى أقراص DVD أو الأقراص المضغوطة. تأكد أن الأقراص قابلة للكتابة والتي تعني أنه بإمكانك إضافة إلى المحتوى، أو حذفه، أو تغييره. في حالة الاعتزام على استخدام هذه الطريقة ويوجد كثير من الملفات المراد نسخها، يجب التأكد أن لديك أقراصاً كافية لإنهاء الوظيفة. يقوم "معالج النسخ الاحتياطي للملفات" بإعلامك بكمية المساحة التي تحتاج إليها كل مرة تقوم فيها بإجراء النسخ الاحتياطي و التوصيات الخاصة بنوع الوسائط المستخدمة. إذا قمت بوضع علامة للأقراص مع تاريخ النسخ الاحتياطي ووقته، هذا الأمر سيسهل العثور عليهم بعد ذلك.

للحصول على الحماية القصوى، عليك الاحتفاظ بالقرص الثابت الخارجي في أحد المواقع المضادة للحريق المنفصلة عن الكمبيوتر.

حيث عند القيام بنسخ الملفات على أحد الأقراص المضغوطة أو أقراص DVD أو القيام بحفظ نسخة على أحد الأقراص الثابتة الخارجية، يلزم تحديد كل ملف ومجلد تريد نسخه احتياطياً يدوياً في كل مرة تريد فيها تنفيذ إحدى عمليات النسخ الاحتياطي. يلزم أيضاً أن تتذكر ضرورة القيام بالنسخ الاحتياطي للملفات والمجلدات الجديدة أو التي تم تعديلها بشكل منتظم. يمكن أن يكون هذا الأمر مستهلكاً للوقت ومملاً. أما عندما تستخدم 'معالج النسخ الاحتياطي للملفات'، فإن Windows يستمر في تعقب الملفات والمجلدات الجديدة أو التي تم تعديلها. وعند القيام بإنشاء إحدى النُسخ الاحتياطية الجديدة، يمكنك إجراء النسخ الاحتياطي لكافة البيانات الموجودة على الكمبيوتر أو الملفات التي تم بتغييرها فقط منذ آخر مرة قمت فيها بإنشاء إحدى النُسخ الاحتياطية. إذا قمت بإعداد النُسخ الاحتياطية التلقائية، يقوم Windows بنسخ الملفات والمجلدات احتياطياً وبشكل منتظم، ولذا ليس عليك تذكر موعد تنفيذ هذه العملية.

٤.٣ - مواقع الشبكة :

إذا كان الكمبيوتر الخاص بك موجوداً على شبكة، يمكنك إجراء النسخ الاحتياطي لموقع على الشبكة. تأكد من أن لديك الأذونات الصحيحة للوصول للشبكة ومن أن المستخدمين الآخرين لا يمكنهم الوصول للنُسخ الاحتياطية التي تنوي إجرائها.

٥ - الملفات التي يجب نسخها احتياطيا :

يجب إجراء نسخ احتياطي لأي شيء يكون من الصعب أو من المستحيل استبداله، فضلاً عن النسخ الاحتياطي بشكل منتظم للملفات التي تقوم بتغييرها بشكل متكرر. تعد الصور وملفات الفيديو والموسيقى والمشاريع والسجلات المالية أمثلة للملفات التي يجب نسخها احتياطياً. لا يلزم نسخ البرامج احتياطياً، نظرًا لأنه يمكنك استخدام أقراص المنتج الأصلية لإعادة تثبيتها ولأن البرامج عادةً ما تشغل جزءاً كبيراً من مساحة القرص.

٦ - أنواع الملفات التي لا يتم تضمينها في النُسخ الاحتياطية :

يقوم 'معالج النسخ الاحتياطي للملفات' بالنسخ الاحتياطي لأكثر أنواع الملفات شيوعاً. لا يتم تضمين الملفات التالية:

•الملفات التي تم تشفيرها باستخدام 'نظام تشفير الملفات' (EFS)

ملاحظةإذا كنت تقوم بتشغيل Windows Vista Service Pack 1، فسيتم تضمين ملفات EFC المشفرة في النُسخ الاحتياطية. ولا يتم تضمين نظام الملفات EFS في Windows Vista Starter، و Windows Vista Home Basic، و Windows Vista Home Premium.

- ملفات النظام (الملفات التي يحتاج Windows تشغيلها).
- ملفات البرامج.
- الملفات المخزنة على الأقراص الثابتة التي يتم تهيئتها باستخدام نظام الملفات FAT.
- البريد الإلكتروني المستند إلى ويب والذي لا يتم تخزينه على القرص الثابت.
- الملفات الموجودة في سلة المحذوفات.
- الملفات المؤقتة.

٧- مشاكل تعذر رؤية الموقع الذي أرغب في النسخ الاحتياطي إليه في معالج 'النسخ الاحتياطي للملفات' :

عندما تختار أحد المواقع لحفظ النسخة الاحتياطية فيه، يبحث المعالج في الكمبيوتر ويعرض قائمة بكافة المواقع التي يمكنك استخدامها. إذا لم يظهر الموقع الذي تريد أن تستخدمه في القائمة، يمكن أن يرجع ذلك إلى إحدى المشاكل التالية :

• يمثل هذا الموقع أحد محركات الشرائط. حيث يتعذر حفظ النُسخ الاحتياطية على الشرائط.

• يمثل هذا الموقع القرص الذي تحاول نسخه احتياطياً. لا يمكنك نسخ القرص احتياطياً على نفس القرص.

على سبيل المثال، لا يمكنك النسخ الاحتياطي لمحتويات محرك الأقراص 'E' على محرك الأقراص 'E'.

• يمثل هذا الموقع أحد محركات الأقراص المضغوطة. يتعذر عليك استخدام أحد محركات الأقراص المضغوطة لإنشاء نسخة احتياطية؛ يجب استخدام إحدى ناسخات الأقراص المضغوطة، التي تُعرف أيضاً بمحرك أقراصCD-R أو CD-RW.

• يمثل هذا الموقع أحد محركات أقراص USB المحمولة. حيث يتعذر حفظ النُسخ الاحتياطية على أحد محركات الأقراص المحمولة.

• لم يتم تنسيق الموقع بتنسيق NTFS أو FAT أو بالتنسيق العام للأقراص المضغوطة (UDF) (والذي يطلق عليه أيضاً نظام الملفات الحيوي). يمكن فقط حفظ النُسخ الاحتياطية على الأقراص التي يتم تهيئتها باستخدام أنظمة الملفات NTFS أو FAT أو UDF. لمزيد من المعلومات، راجع المقارنة بين نظامي الملفات NTFS وFAT.

• الموقع إما أن يكون قرص النظام (القرص الذي تم تثبيت Windowsعليه—يسمى أيضاً بـ محرك الأقراص C) أو قرص

التمهيد (القرص الذي يستخدمه Windows لبدء تشغيل الكمبيوتر—يسمى أيضًا بـ قرص بدء التشغيل).

• أو يمثل الموقع مشاركة الشبكة على الكمبيوتر الذي يقوم بتشغيل Windows XP Home Edition. يتعذر حفظ النُسخ الاحتياطية في مواقع المشاركات هذه لأن Windows XPHome Edition لا يدعم تعيين الأذونات لأي مشاركات على الشبكة ولا المصادقة عبر الشبكة.

حيث يتعذر عليك الحصول على نُسخ للملفات الموجودة على أحد الأقراص المفقودة. مع ذلك، يمكنك استعادة الملفات الموجودة على أقراص النسخ الاحتياطي التي تم إنشاؤها قبل القرص المفقود أو بعده. إذا كنت لا تعرف بالضبط ما الذي يوجد على القرص المفقود، يمكنك مشاهدة قائمة بالملفات التي قمت بنسخها احتياطياً.

الوحدة الثالثة

طرق التحكم في
الوصول للشبكة

مقدمة:

في الماضي كانت الحواسب مستقلة عن بعضها البعض و كان يتم وضعها في مراكز كبيرة تدعى مراكز معلومات وكان يتم حماية هذه المركز من هجمات العالم الخارجي بواسطة قفل الأبواباً و مع انتشار الشبكات انتشارا واسعا أصبح إغلاق الأبواب و وضع الأقفال غير كافيا لحماية الحاسوب معلوماته من الاختراق لأن الهجمات ستأتي الآن من الشبكة أي من أي حاسب آخر و قد يكون حتى من دولة أخرى.إن تحقيق الأمن لشبكة خاصة في ظل انتشار و توسع الانترنت أمر صعب و خاصة أن الانترنت الآن تعج بالمواقع و خاصة مواقع الهاكرز وأدواتهم بشكل مجاني.

١ - الحاجة لسياسة أمن الشبكة :

إن أول خطوة في كتابة أي سياسة أمنية هو تحليل المخاطر و دراستهاً إن تحليل المخاطر يعني دراسة ماذا تريد أن تحمي ضمن شبكتك و من ماذا تريد حمايته و كيف ستتم حمايته أوهذا يعني تحديد المخاطر و وضعها ضمن مستويات و درجات و طرق تجنبها و مواجهتها عند حدوثها.

١,٢ـ كيف نحقق الأمن للشبكة :

١,٢,١ـ أهداف سياسة الشبكة :

إن هدف هذه السياسة هو حماية موارد الشبكة و موارد الموظفين و عملهم من وصول المخربين و من وصول الأشخاص غير المخول لهم

مما قد يسبب سوء استعمال أو ضياع للمعلوماتأ و يتحقق ذلك من خلال الأمور التالية :

١.٢.١.١ – إتاحة الموارد للمستخدمين الموثقين فقط.

١.٢.١.٢ – تحقيق التكاملية لأنظمة الشبكة من الضياع أالمخاطر التي قد تحدث بسبب الدخول غير المخول له للشبكة.

١.٢.١ – يتم تحقيق الأمرين السابقين من خلال :

- تفويض مسؤوليات الأمن لطيف واسع من المستويات.
- تحديد الحد الأدنى لمتطلبات الأمن.
- تحديد الإجراءات اللازم اتخاذها للحفاظ على الأمن.

١.٣ – **أفق السياسة الشبكية** :

يتم تحديد أفق هذه السياسة من خلال الإجابة عن الأسئلة الأربعة التالية :من أما ألماذا أكيف.

١.١.٣ – **من هو المسؤول:**

إن كل شخص في المؤسسة و كل شخص يستخدم الشبكة هو شخص مسؤول عن الأمن في المؤسسة .يقوم المركز الرئيسي فقط بالدعم التقني اللازم لتحقيق الأمن في الشبكات ذات المستخدمين العديدين أليس من المعقول أن نطالب بـأمن عام للمؤسسة دونت أن نطلب من كل شخص على حدا أن يحقق أمنه الخاص و حماية جهازه و بياناته من الضياع.

٢- المسؤولية :

تنقسم المسؤولية إلى قسمين:

٢.١- المركز الرئيسي :

حيث يحتوي على النظام الرئيسي للمؤسسة أي السيرفر وفيه يتم تحديد السماحيات للمستخدمين إن هذه الأنظمة عادة ما تكون ذات مواصفات عالية و يتم عليها حفظ بيانات المؤسسة و القيام بالمعالجات اللازمة.

٢.١.١- مسؤوليات المركز الرئيسي :

٢.١.١.١- صيانة النظام : شمل الصيانة تحديث البرامج و تحديث الموارد و تحديث السماحيات.

٢.١.١.٢- إدارة السرية : إنشاء مستخدمين جدد و منحهم السماحيات و وضع سياسات أمنية جديدة.

٢.١.١.٣- التوثيق : يجب أن يكون المركز الرئيسي مسئولا عن التوثيق لكل الخطوات و الاجرائيات التي تتم ضمن الشبكة و التوثيق له نوعان شخصي و آلي بحيث يشمل كل حركة في الشبكة

٢.٢- أنظمة الاتصال :

ويعني الشبكة المسؤولة عن ربط أجهزة المستخدمين معا و تأمين الاتصال و تبادل المعلومات ضمن فروع المؤسسة داخليا و بين فروعها و المحيط الخارجي أو مع شبكة خارجية

يجب أن تكون السياسة الآنية للمؤسسة واضحة و معروفة من قبل الجميع إن الوضوح يعني:

تقسيم و توزيع المسؤوليات التي تؤمن الحماية على جميع الموظفين و تقسيمهم لمستويات.

- كتابة الإجراءات اللازمة و شرحها بشكل واضح لتحقيق و تنفيذ السياسة.
- تحديد المتطلبات التقنية التي تلزم لتحقيق أمن على سوية كبيرة.

٣- السياسة الشخصية:

يحدد هذا القسم السياسة الشخصية لكل مستخدم لديك على الشبكة و ما هي السماحيات التي يملكها على موارد الشبكة مثل الطابعة و الانترنت و يجب تحديد السماحيات بدقة مثل سماحيات استخدام الألعاب باستخدام البريد الالكتروني تصفح الانترنت و استخدام ما سبق للفائدة الشخصية.

٤ – لماذا نحتاج إلى أمن الشبكة وحمايتها في المؤسسات :

٤.١ – حماية الموارد:

و يقصد بالموارد أجهزة الموظفين أ أجهزة الاتصال أ المعلومات المخزنة أو تلك التي يتم معالجتها .إن ضياع معلومات ما أو فقدان الوصول لجهاز ما يعني ببساطة ضياعا في الجهد و بالتالي ضياعا في المال . تخيل فقدان قاعدة بيانات ضخمة تحوي مشاريع الطلاب في كلية ما أو ضياع قاعدة

بيانات إدخال أسماء المواطنين في السجل المدني لدولة ما أبالمحصلة من وجهة نظر اقتصادية إن ضياع أي معلومة يعني جهدا إضافيا مبذولا و يعني دفع رواتب إضافية نحن بغنى عنها.

٤.١.١ - حيث يمكن أن يشمل الضرر:

- وصول مخربين للمعلومات
- نشر المعلومات لشركات منافسة
- ضياع المعلومات أو حذفها

٤.٢ - الالتزامات القانونية:

في المشاريع الحكومية الضخمة لا مجال للخطأ و يتوجب تحقيق الأمن بأعلى مستوياته و كذلك الحال في المشاريع الموازية مثل البنوك.

٤.٣ - السمعة و الثقة :

إن ضياع معلومات لزبائنك يؤدي لتهديد سمعتك في السوق و ابتعاد الزبائن عنك حتى و لو قمت بإقناعهم أن الخطأ غير مقصود أو نتيجة قضاء و قدر أو أنه كان عبارة عن عمل إجرامي و غير أخلاقي و حتى لو دفعت لهم التعويضات المجزية فإن ذلك سيؤثر على سمعتك و لعل البنوك هي أوضح مثال على ذلك.

٤.٤ - الحماية من التهديدات :

تأتي التهديدات للمؤسسة من داخل المؤسسة أو خارجها و قد تكون هذه التهديدات هي عبارة عن :

• مجرد ألاعيب .

• هاكر فضولي .

•أخطاء برمجية غير معروفة.

• أخطاء قاتلة للموظفين.

• أخطاء غير مقصودة.

٥ - حماية البيانات والمعلومات من النفاذ غير مشروع :

٥.١ - الحماية من التخريب :

في بعض الأحيان يمكن أن تصادف بعض المستخدمين غير الحذرين الذين يمكن أن يحذفوا مئات الملفات بالخطأ، وقد تكون هذه الملفات تحمل بيانات في غاية الأهمية.

٥.٢ - المحافظة على السرية :

قد تجد بعض موظفين شركة معينة يحبون التطفل وفتح وقراءة ملفات الغير الشخصية.

٥.٣ - الحماية من اللصوصية :

قد تجد بعض المستخدمين ضعفاء النفوس الذين بإمكانهم النفاذ إلى حسابات الشركة واستخراج شيكات بأسمائهم مما يتسبب في خسائر للشركة.

٥.٤ - الحماية من التخريب المتعمد :

يمكن لأحد مستخدمين الشبكة المتذمرون والذي يملك النفاذ إلى ملفات الشبكة أن يدمرها أو يغير فيها والى أن يكشف هذا التخريب يمكن أن تقع الشبكة في مأزق مالي معقد للغاية.

٦ـ متطلبات الأمان في الشبكة :

٦,١ـ المتطلبات التقنية :

يجب أن تتوفر القدرات التقنية بالحد الأدنى الذي يحقق دعم و حماية مستخدمين الشبكة و مواردهم.

٦.٢- متطلبات النظام :

من أجل أي نظام متعدد المستخدمين يلزم حماية و تحقيق ما يلي :

٦.٢.١- حماية المعرفات للمستخدم ID :

يجب أن يكون لكل موظف معرف خاص به بحيث يقوم بالتعريف عن المستخدم عندما يقوم بدخول و استخدام مورد ما و بالتالي يتم اختبار فيما إذا كان الشخص مسموحا له باستخدام المورد أو لا .يجب حماية هذا المعرف بحيث لا يستخدمه سوى صاحبه و بالتالي يجب إيجاد آلية للحماية قد تكون برمجية من خلال استخدام كلمة سر أو هاردوير أو من خلال بطاقات ممغنطة مثلا.

٦.٢.٢- حماية موارد المستخدم :

و يجب أن يتم تحديد مالك كل مورد و عادة ما يكون المورد عبارة عن قاعدة بيانات قرص مرن قرص صلب ...الخ و يجب أن يتم منح

الوصول و التحكم لمالك المورد فقط دون غيره و أن يمنع وصول غير المالكين له و طبعا يتم ذلك من خلال إعطاء سماحيات للمستخدمين حسب أرقام معرفاتهم و غالبا ما يتم تطبيق السماحيات و المنع على مجموعة من المستخدمين معا . يجب أن يكون هناك حلول وسط مثل إمكانية القراءة من قاعدة بيانات دون السماح بتعديلها.

٦.٢.٣- حماية موارد الأنظمة :

إن موارد النظام ككل أكبر من مجرد مورد لمستخدم معين فالنظام ككل يقوم بعمل كل شيءأو هذه الموارد تكون ثمينة و غالية حيث تشمل قواعد البيانات الرئيسيةأالمعالجاتأالطباعةأبرامج النظام و لذلك يجب أن تكون هناك سياسة واضحة عند التعامل مع هذه الأنظمةأفمثلا يجب السماح للمستخدمين باستخدام مورد ما مثل الطابعة و لكن لا يسمح لهم بإطفاء الحاسب أو إعادة إقلاعه.

٦.٣- متطلبات التحكم :

- للتحكم نوعين:

٦.٣.١- تحكم موزع :

يتم توزيع التحكم على جميع المستخدمين المالكين لمورد ما و كل مستخدم يتحكم بمورده بشكل مستقل و كل تحديث يقوم به المدير أو المستخدم يطبق مباشرة.

٦.٣.٢- وصول محدد :

يقوم المستخدم بالوصول و تحديث مورد ما حسب السماحيات التي يمتلكها.

٦.٤- التقارير :

يجب أن يكون النظام قادرا على تسدي و كتابة التقارير المفصلة عن كل السماحيات و تحديثاتها و التي قام بها المدراء و كما يتم تسجيل محاولات الاختراق و حالات الاختراق ضمن التقارير.

٦.٥- الاستعادة :

يجب أن يكون النظام قادرا على استعادة حالة العمل إلى مرحلة سابقة تم حفظها بالنسخ الاحتياطي.

٦.٦- متطلبات الاتصالات :

٦.٦.١- التحكم بالوصول :

يجب أن يكون نظام الاتصالات قادرا على عزل جزء من الشبكة عن العالم الخارجي أو استعادة الاتصال بين موقع محلي و بقية النظام بدون التأثير على الاتصالات بين العقد الأخرى على الشبكة.

٦.٦.٢- التقارير:

يجب أن يكون نظام الاتصالات قادرا على تسجيل و كتابة التقارير التي تراقب كل شيء متعلق بالشبكة كزيادة عرض الحزمة المستهلكة و الضغط على الشبكة و معدل نقل و تراسل البيانات بين العقد الداخلية و الخارجية.

٦.٧- نماذج الأمان:

في أنظمة التشغيل التي تعتمد على شبكة عميل / ملقم تخزن حسابات المستخدمين في موقع مركزي يكون عليه خدمة الدليل :

(Active Directory) في شبكات Windows

(Novell Directory Services) في شبكات Novell NetWare.

٦.٧.١- الأمان على مستوى المستخدم وعلى مستوى المشترك.

على شبكات الند - ند (Peer to Peer) يحتفظ كل كمبيوتر بمعلومات الأمان الخاصة به ويقوم بعمليات المصادقة الخاصة به .

يمكن أن تعمل الكمبيوترات كعملاء وملقمات في نفس الوقت أوحين يحاول عميل أن يستخدم موارد على جهاز آخر يعمل كملقم أيقوم العميل بالمصادقة قبل منحه حق الوصول .

يوجد نوعان أساسيان لنماذج الأمان المستخدمة في Windows ومعظم أنظمة التشغيل الأخرى هما :

*الأمان على مستوى المستخدم.(User Level Security)

*الأمان على المستوى المشترك(Share Level Security)

٦.٧.١.١- الأمان على مستوى المستخدم :

هي أذونات لمستخدمين معينين لكيفية استخدام موارد الشبكة.

ويعتبر أكثر أمان من المستوى المشترك بمراحل.

6.7.1.2- الأمان على المستوى المشترك:

هي تعيين كلمات مرور للموارد المشتركة المختلفة التي ينشئونها على الكمبيوترات لديهم.

لا يعطي الكثير من الحماية لأنه يمنح الجميع نفس كلمة المرور للوصول إلى موارد الشبكة . وميزة الأمان على المستوى المشترك أن أي مستخدم بغض النظر عن خبرته يستطيع أن يتعلم كيف يعد كلمات مرور خاصة لموارده المشتركة مما يقلل المتابعة المستمرة من مسئول الشبكة.

٨- ضبط المهام المسموح بها للمستخدمين :

- إعطاء تصاريح Permissions للمستخدمين للوصول للبيانات و المعدات كل حسب طبيعة عمله و في هذه الحالة يجب مشاركة البيانات و المعدات للسماح للآخرين باستخدامها.

- تزويد المستخدمين بحقوق Rights تحدد الأنشطة و العمليات المسموح لهم إجراءها على النظام.

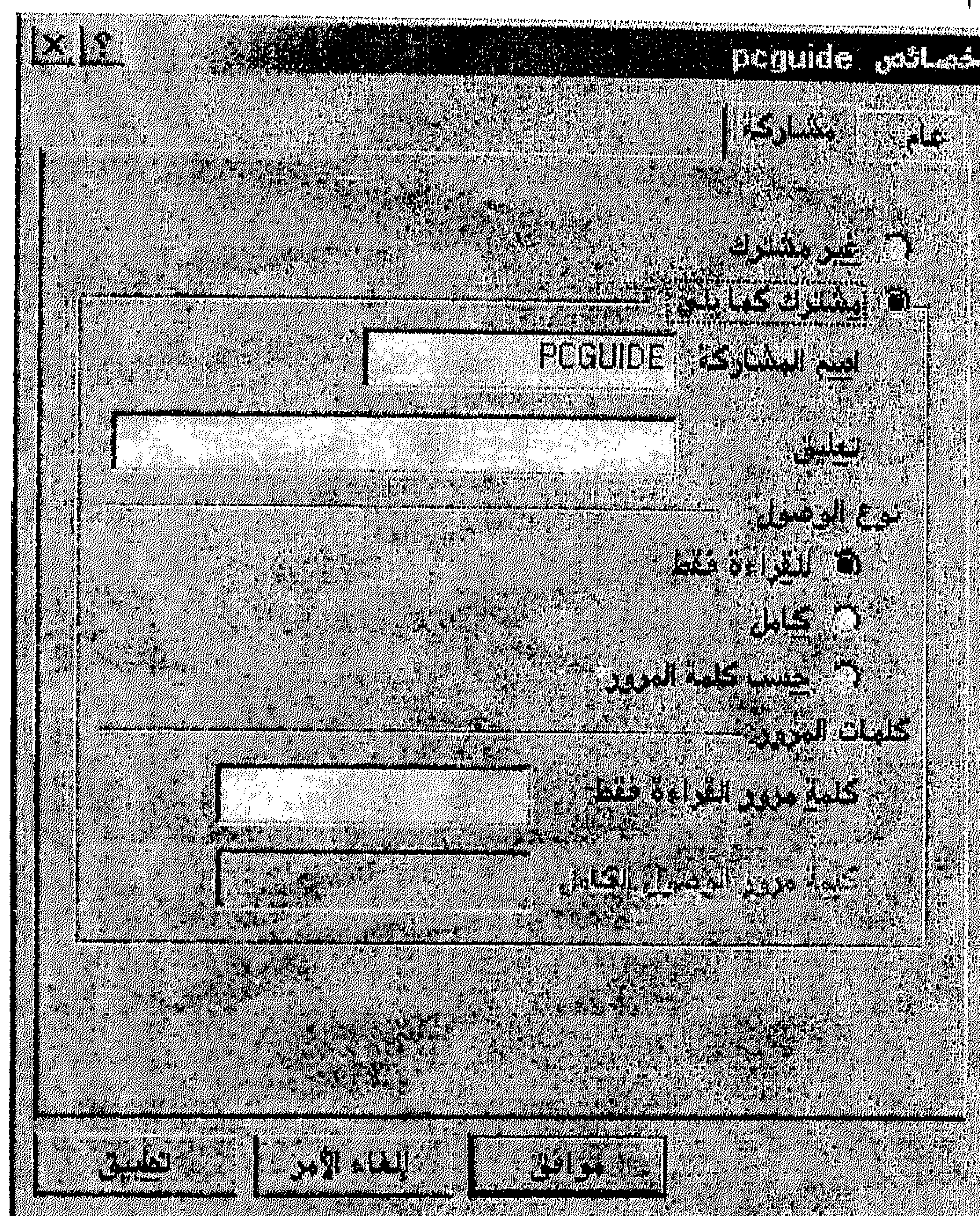
٨.١- هناك نظامان أساسيان لإعطاء التصاريح و الحقوق :

٨.١.١- المشاركة المحمية بكلمة مرور.

٨.١.٢- تصاريح الوصول.

في النظام الأول يتم تعيين كلمة سر لكل من الموارد المطلوب مشاركتها و يتم الوصول لهذه الموارد فقط من قبل من لديه كلمة السر.

كما تستطيع تحديد درجة الوصول هل هي للقراءة فقط أم وصول كامل أم وفقا لكلمة السر .أنظر الصورة.



في النظام الثاني يتم تعيين الحقوق و إعطاء التصاريح لكل مستخدم أو مجموعة مستخدمين ، و يكفي أن يدخل المستخدم كلمة المرور عند الدخول الى نظام التشغيل ليتعرف النظام على حقوق هذا المستخدم و التصاريح المتوفرة له، و يعتبر هذا النظام أكثر أمنا من النظام السابق و يعطي مدير الشبكة تحكما أكبر بكل مستخدم.

عند إدخال الاسم و كلمة المرور يتم تمرير هذه المعلومات الى مدير أمن الحسابات SAM (Accounts Manager Security) فإذا كان الولوج إلى جهاز Workstation فإن المعلومات يتم مقارنتها مع قاعدة بيانات حسابات الأمن المحلية في الجهاز، أما إذا كان الولوج الى نطاق Domain فإن المعلومات يتم إرسالها الى مزود SAM الذي يقارنها مع قاعدة بيانات حسابات النطاق، فإذا كان اسم المستخدم أو كلمة المرور غير صالحين فإن المستخدم يمنع من الدخول الى النظام، أما إذا كانا صحيحين فإن نظام الأمن الفرعي يقوم بإصدار بطاقة ولوج Access Token تعرف النظام بالمستخدم فترة ولوجه و تحتوي هذه البطاقة على المعلومات التالية:

١- المعرف الأمني SID (Security Identifier) و هو رقم فريد خاص بكل حساب.

٢- معرفات المجموعة Group SIDs و هي التي تحدد المجموعة التي ينتمي لها المستخدم.

٣- الامتيازات Privileges و هي تمثل الحقوق الممنوحة لحسابك.

كما أنه يتم إصدار Access Token عند محاولتك الاتصال من جهازك بجهاز آخر على شبكتك و يطلق على هذا الإجراء الولوج عن بعد Remote Logon.

من الأمور التي يجب مراعاتها عند الحديث عن أمن الشبكة هو المحافظة على أمن الموارد مثل الطابعات و محركات الأقراص و الملفات و التي يقوم مدير الشبكة بتعيين تصاريح لاستخدام هذه الموارد.

٨.٢- ومن التصاريح التي قد تعطى للوصول إلى الملفات ما يلي :

١ - تصريح قراءة و يسمح لك بعرض و نسخ الملفات.

٢- تصريح تنفيذ للتطبيقات.

٣- تصريح كتابة و يسمح بالتعديل في محتوى الملفات.

٤ - ممنوع الاستخدام No Access.

و التصاريح ممكن منحها لمستخدم أو مجموعة من المستخدمين و هذا إسهل.

يمتلك كل مورد من الموارد قائمة تحكم بالوصول Access Control (List) ACL و كل معلومة يتم إدخالها في ACL يطلق عليها ACE (Access Control Entry).

يتم إنشاء ACE عند منح التصريح لإستخدام المورد و تحتوي على SID للمستخدم أو مجموعته الممنوحة التصريح بالإضافة الى نوع التصريح، فلو افترضنا أن مدير مجموعة ما قد مُنح تصريح قراءة و تصريح كتابة لملف ما فإن ACE جديد يتم إنشاؤه ثم إضافته الى ACL الخاص بالملف و سيحتوي ACE على SID لمدير المجموعة بالإضافة الى تصريح قراءة و تصريح كتابة.

هناك نوعان ل- ACE :

١- الوصول مسموح Access Allowed.

٢- الوصول ممنوع Access Denied و يتم إنشاؤها إذا كان تصريح الوصول هو No Access.

و هكذا عندما يحاول مستخدم ما الوصول الى مورد ما يتم مقارنة SID الخاص به مع SIDs في كل ACE من ACL للمورد.

في ويندوز NT و ويندوز ٢٠٠٠ يتم ترتيب ACE بحيث تكون Access Denied ACEs قبل Access Allowed ACEs ، فإذا وجد SID خاصتك في أي من Access Denied ACEs فستمنع من الوصول الى المورد و إلا فسيبحث في Access Allowed ACEs للتأكد من الحقوق الممنوحة لك فإن لم يعثر على SID مطابق لخاصتك فستعرض رسالة تحذير تمنعك من الوصول للمورد.

الوحدة الرابعة

أنواع فيروسات الحاسب وكيفية مقاومتها

مقدمة

معرفة الفرق بين الدودة والتروجان والفيروس،حيث هناك الكثير لا يمكن التمييز بين هذه المصطلحات.نأتي إلى استعراض الفروقات بين هذه المصطلحات :

• الدودة:

تصيب الدودة الكمبيوترات الموصلة بالشبكة بشكل أوتوماتيكي و من غير تدخل الإنسان وهذا الأمر يجعلها تنتشر بشكل أوسع وأسرع عن الفيروسات . الفرق بينهم هو أن الديدان لا تقوم بحذف او تغيير الملفات بل تقوم بتهليك موارد الجهاز واستخدام الذاكرة بشكل فظيع مما يؤدي إلى بطء ملحوظ جدا للجهاز أومن المهم تحديث نسخ النظام المستخدم في الجهاز كي يتم تجنب الديدان.

ومن المهم عند الحديث عن الديدان الإشارة إلى تلك التي تنتشر عن طريق الإيميل. حيث يرفق بالرسالة ملفاً يحتوي على دودة، و عندما يشغّل المرسل إليه الملف المرفق، تقوم الدودة بنشر نفسها إلى جميع الإيميلات الموجودة في دفتر عناوين الضحية.

• التروجان:

وهو عبارة عن برنامج يغري المستخدم بأهميته أو بشكله أو باسمه إن كان جذاباً و في الواقع هو برنامج يقوم بفتح باب إن صح التعبير بمجرد تشغيله أو من خلال هذا الباب يقوم المخترق باختراق الجهاز وبإمكانه التحكم بالجهاز بشكل كبير حتى في بعض الأحيان يستطيع القيام بأمور

أ صاحب الجهاز نفسه لا يستطيع القيام بهاأ و هذا لا يرجع لملف التروجان لكن ملف التروجان هو الذي فتح للمخترق الباب إن صح التعبير بتشغيله إياه.

الفيروس:

• كما ذكرناأ الفيروس عبارة عن برنامج صمم لينشر نفسه بين الملفات و يندمج او يلتصق بالبرامج. عند تشغيل البرنامج المصاب فانه قد يصيب باقي الملفات الموجودة معه في القرص الصلب او المرنأ لذا الفيروس يحتاج إلى تدخل من جانب المستخدم كي ينتشرأ بطبيعة الحال التدخل عبارة عن تشغيله بعد أن تم جلبه من الإيميل أو تنزيله من الانترنت أو من خلال تبادل الأقراص المرنة.

١ - تعريف الفيروس :

يوجد تعريفان للفيروس هما :

- الفيروس عبارة عن كود برمجي الغرض منها إحداث أكبر قدر من الضرر. ولتنفيذ ذلك يتم إعطاؤه القدرة على ربط نفسه بالبرامج الأخرى عن طريق التوالد والانتشار بين برامج الحاسب وكذلك مواقع مختلفة من الذاكرة حتى يحقق أهدافه التدميرية.

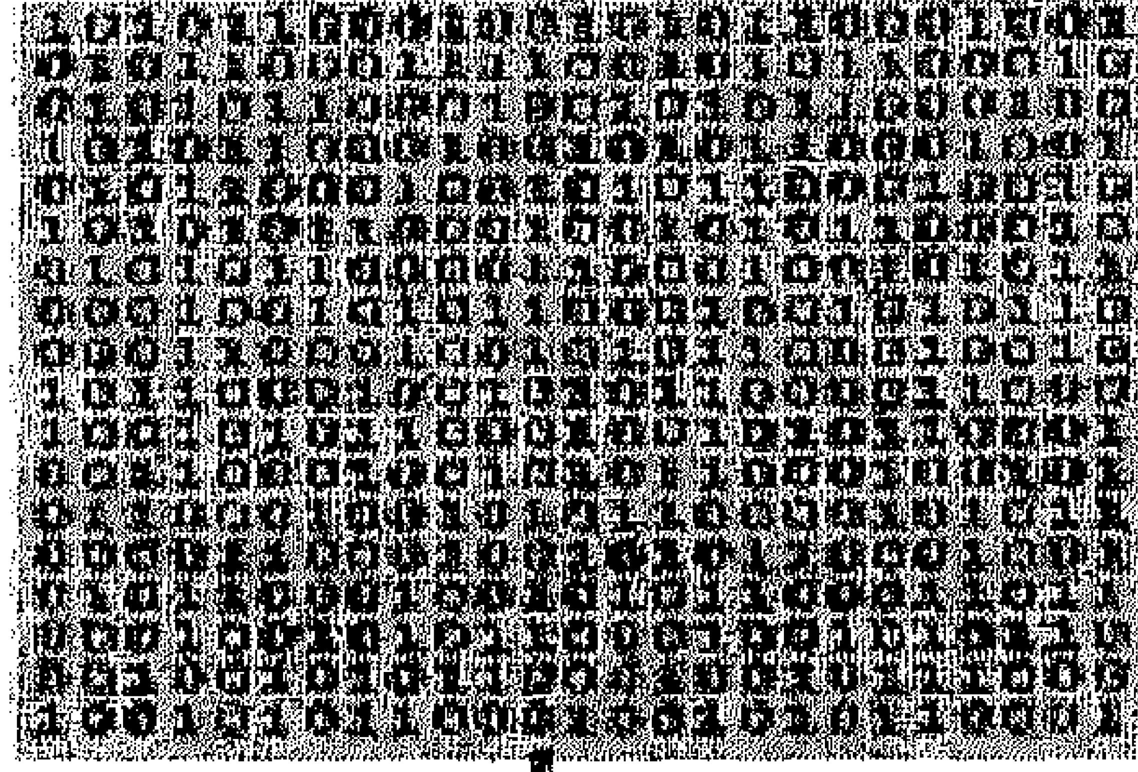
- الفيروس عبارة عن برنامج تطبيقي يصممه أحد المخربين لتدمير البرامج والأجهزة. والتعريف الأول لأن الفيروس لا يستطيع أن يعمل بمفرده دون وسط ناقل.

١.١ - كيف يعمل الفيروس :

يحاول كل فيروس تقريباً أن يقوم بنفس الشيء. وهو الانتقال من برنامج إلي آخر ونسخ الكود إلي الذاكرة ومن هناك يحاول الكود نسخ نفسه إلي أي برنامج يطلب العمل أو موجود بالفعل قيد العمل، كما يحاول هذا الكود أن يغير من محتويات الملفات ومن أسمائه أيضاً دون أن تعلم نظام التشغيل بالتغيير الذي حدث، مما يتسبب في فشل البرامج في العمل. ويعرض أيضاً رسائل مزعجة ومن ثم يخفض من أداء النظام أو حتى يدمر النظام كاملاً. وهناك بعض الفيروسات التي تلتقط عناوين البريد الإلكتروني ثم تؤلف رسائل نيابة عنك وترسلها إلي جميع العناوين الموجودة في مجلد العناوين لديك مرفقة بملفات ملوثة بالفيروس.

في الواقع يقوم الفيروس في حالة إصابة الملف بإضافة نفسه في بداية أو نهاية الملف المصاب، دون أن يقوم فعلياً بأي تغيير في مكوّنات الملف الأصلية. لننظر للصورة التالية التي توضّح شكل البرنامج غير المصاب بفيروس.

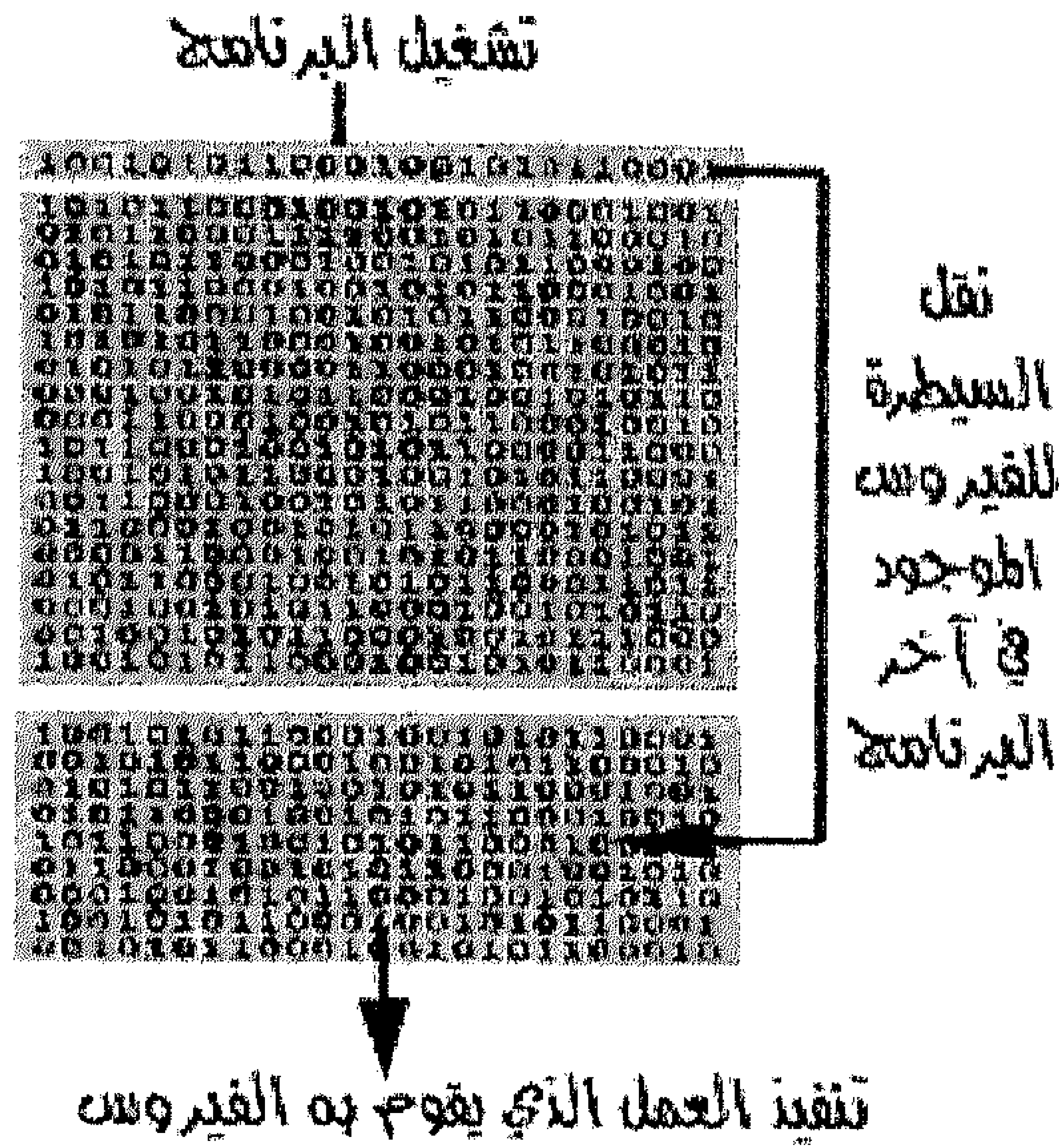
تشغيل البرنامج



تنفيذ البرنامج

نلاحظ أنه عند استدعاء البرنامج فإنه يعمل بشكل طبيعي.والآن لنتصوّر أنه تم اصابة البرنامج بفيروس. في الواقع يقوم الفيروس بلصق نفسه في البرنامج كما أسلفنا دون أن يغير في محتويات الملف شيئاً. وطريقة اللصق تكون، إما أنه يقوم بلصق نفسه في بداية البرنامج، بحيث يتم تشغيله هو قبل البرنامج نفسه:

وقد تكون طريقة التحاق الفيروس بالملف بأن يضع نفسه في نهاية البرنامج المصاب. و يضع علامة في بدايته، هكذا:



إن هذا الفيروس، يختبئ في نهاية الملف المصاب، و يضع في مقدّمة البرنامج مؤشّراً بحيث أنه عندما يتم استدعاء البرنامج و تشغيله، يحوّل السيطرة للفيروس بدلاً من تشغيل البرنامج.

وفي الحالتين قد يعود الفيروس بعد الانتهاء من تنفيذ عمله المؤذي لتشغيل البرنامج، و لكنه قد لا يعود أيضاً. و يسبب أضراراً جسيمة للجهاز.

١.٢- شروط الفيروس :

١- أن يكون ذا حجم صغير لكي لا يتم الانتباه إليه.

٢- أن يعتمد على نفسه في التشغيل أو على البرامج الأساسية أو عن طريق الارتباط بأحد الملفات.

٣- أن يكون ذا هدف ومغزى.

٢- العوامل التي أدت إلي سرعة انتشار الفيروسات :

٢.١- التوافقية Compatibility وتعني قدرة البرنامج الواحد على أن يعمل على حاسبات مختلفة وعلى أنواع وإصدارات مختلفة من نظم التشغيل، وهذا العامل رغم تأثيره الإيجابي والهام بالنسبة لتطوير الحاسبات إلا أن أثره كان كبيراً في سرعة انتشار الفيروسات. كما ساعدت أيضاً البرامج المقرصنة على سرعة انتقال الفيروسات.

٢.٢- وسائل الاتصالات Communications كان لوسائل الاتصالات الحديثة السريعة دور هام في نقل الفيروسات. ومن أهم هذه الوسائل: الشبكات بما فيها شبكة الإنترنت. وإلا لما استطاع فيروس الحب أن يضرب أجهزة في أمريكا رغم أن مصدره الفلبين.

٢.٣- وسائط التخزين مثل الأقراص المرنة Floppy والأقراص المضغوطة CD خاصة إذا كانت صادرة عن جهاز مصاب.

٣ـ خصائص الفيروسات :

٣,١ـ القدرة على التخفي :

للفيروسات قدرة عجيبة على التخفي والخداع عن طريق الارتباط ببرامج أخرى. كما تم أيضاً تزويد الفيروسات بخاصية التمويه والتشبه. حيث أن الفيروس يرتبط ببرنامج يقوم بأعمال لطيفة أو له قدرة عرض أشياء مثيرة وعند بداية تشغيله يدخل إلي النظام ويعمل على تخريبه.

وللفيروسات عدة وسائل للتخفي منها ارتباطها بالبرامج المحببة إلي المستخدمين. ومنها ما يدخل النظام على شكل ملفات مخفية بحيث لا تستطيع ملاحظة وجوده عن طريق عرض ملفات البرنامج. وبعض الفيروسات تقوم بالتخفي في أماكن خاصة مثل ساعة الحاسب وتنتظر وقت التنفيذ. كما أن بعضها تقوم بإخفاء أي أثر لها حتى أن بعض مضادات الفيروسات لا تستطيع ملاحظة وجودها ثم تقوم بنسخ نفسها إلي البرامج بخفة وسرية.

٣.٢- الإنتشار:

يتميز الفيروس أيضاً بقدرة هائلة على الانتشار سواء من ناحية السرعة أو الإمكانية.

٣.٣- القدرة التدميرية:

تظهر عندما يجد الفيروس المفجر الذي يبعثه على العمل كأن يكون تاريخ معين كفيروس تشرنوبيل.

٤- أنواع الفيروسات:

٤,١- فيروسات قطاع التشغيل Boot Sector :

تعتبر الفيروسات التي تصيب مقطع التشغيل في الأقراص أكثر انتشاراً في العالم، إذ تصيب المقطع التشغيلي في الأقراص المرنة، أو مقطع نظام تشغيل "DOS" في الأقراص الصلبة. وربما إذا عرفنا كيف تنتشر هذه الفيروسات أمكننا أن نتقي شرها. لقد وصلك اليوم قرص مرن يحتوي

على معلومات مهمة لمشروع تعمل عليه مع عدد من الزملاء، وربما لا يعرف زميلك الذي أرسل لك هذا القرص أنه يحتوي على فيروس يصيب المقطع التشغيلي للقرص الصلب بالعطب. ووضعت القرص في محرك الأقراص وبدأت العمل كالمعتاد، وإلي الآن لم يقم الفيروس بأي نشاط يذكر، وأقفلت جهازك بعد أن انتهيت من العمل. وفي اليوم التالي قمت بتشغيل الكمبيوتر وما زال القرص المرن قابعاً داخل الجهاز عندها يحاول الكمبيوتر الإقلاع من القرص المرن. وتبدأ الكارثة حيث يقوم الفيروس بنسخ نفسه في الذاكرة بدلاً من برامج التشغيل المعروفة ويقوم بتشغيل نفسه بعدها. وقد تنتبه إلي وجود القرص المرن وتسحبه من الجهاز وتحاول التشغيل من القرص الصلب وعندها يقوم الفيروس بشطب ملفات الإقلاع الموجودة أصلاً في نظام تشغيل "DOS" ويحل محلها. وإلي هنا يبدو كل شيء طبيعياً، إلي أن تحاول القراءة أو الكتابة من القرص الصلب فلا يمكنك ذلك، ويقوم الفيروس بمخاطبة القرص المرن بنسخ نفسه عليه، وتقوم بكل حسن نية بإعطاء ذلك القرص إلي صديق أو زميل لتتكرر العملية من جديد.

٤.٢ - فيروسات الملفات :

تلصق هذه الفيروسات نفسها مع ملفات البرامج التنفيذية مثل: command.com أو win.com .

٤.٣ - الفيروسات المتعددة الملفات :

تنسخ هذه الفيروسات نفسها في صيغة أولية ثم تتحول إلي صيغ أخرى لتصيب ملفات أخرى.

٤.٥ - الفيروسات الخفية (الأشباح) :

وهذه فيروسات مخادعة. إذ إنها تختبئ في الذاكرة ثم تتصدى لطلب تشخيص وفحص قطاع التشغيل ثم ترسل تقريراً مزيفاً إلي السجل بأن القطاع غير مصاب.

٤.٦ - الفيروسات متعددة القدرة التحولية :

وهذه الفيروسات لها القدرة الديناميكية على التحول وتغيير الشفرات عند الانتقال من ملف إلي آخر لكي يصعب اكتشافها.

٤.٧ - الفيروسات متعددة الأجزاء Multipartite :

يجمع هذا النوع الذي يدعى الفيروس "متعدد الأجزاء" Multipartite بين تلويث قطاع الإقلاع مع تلويث الملفات في وقت واحد.

٤.٨ - فيروسات قطاع الإقلاع :

تقبع فيروسات قطاع الإقلاع في أماكن معينة على القرص الصلب ضمن جهازك، وهي الأماكن التي يقرأها الكمبيوتر وينفذ التعليمات المخزنة ضمنها عند الإقلاع. وتصيب هذه الفيروسات منطقة قطاع الإقلاع الخاصة بنظام (Record DOS, DOS Boot) بينما تصيب

فيروسات الفئة الفرعية المسماه: MBR Viruses، قطاع الإقلاع الرئيسي للكمبيوتر Master Boot Record حيث يقرأ الكمبيوتر كلا المنطقتين السابقتين من القرص الصلب عند الإقلاع مما يؤدي إلي تحميل الفيروس في الذاكرة. يمكن للفيروسات أن تصيب قطاع الإقلاع على الأقراص المرنة، لكن الأقراص المرنة النظيفة والمحمية من الكتابة تبقى أكثر الطرق أمناً لإقلاع النظام في حالات الطوارئ. والمشكلة التي يواجهها المستخدم بالطبع هي كيفية التأكد من نظافة القرص المرن، أي خلوه من الفيروسات قبل استخدامه في الإقلاع وهذا ما تحاول أن تفعله برامج مكافحة الفيروسات.

٤.٩ - الفيروسات الطفيلية:

تلصق الفيروسات الطفيلية Viruses Parasitic نفسها بالملفات التنفيذية، وهي أكثر أنواع الفيروسات شيوعاً. وعندما يعمل أحد البرامج الملوثة فإن هذا الفيروس عادة ينتظر في الذاكرة إلي أن يشغل المستخدم برنامجاً آخر، فيسرع عندها إلي تلويثه. وهكذا يعيد هذا النوع من الفيروس إنتاج نفسه ببساطة من خلال استخدام الكمبيوتر بفعالية أي بتشغيل البرامج! وتوجد أنواع مختلفة من ملوثات الملفات لكن مبدأ عملها واحد.

٤.١٠ - الفيروس المتطور Virus Polymorphic :

هي فيروسات متطورة نوعاً ما تغير (الكود) الشفرة كلما انتقلت من

جهاز إلي آخر. ويصعب نظرياً على مضادات الفيروسات التخلص منها لكن عملياً ومع تطور المضادات فالخطر أصبح غير مخيف.

٤.١١- فيروسات الماكرو:

يعتبر هذا النوع من الفيروسات أحدث ما توصلت إليه التقنية في هذ ا المجال، وغدت تشكل تهديداً كبيراً لأسباب عديدة هي :

١ - تكتب فيروسات الماكرو بلغة Word المتوفرة لكثير من المستخدمين، وهي أسهل من لغات البرمجة التقليدية.

٢ - أول فيروسات من نوعها تصيب ملفات البيانات أكثر من الملفات التنفيذية وهنا يكمن الخطر، حيث أن نسبة تداول ملفات البيانات أكبر بكثير من الملفات التنفيذية إذا أضفنا لذلك أيضاً البريد الإلكتروني وإمكانية إلحاق ملفات البيانات معها، وكذلك الاستخدام غير المحدود لشبكة الإنترنت. لذلك كله يكون خطر فيروسات الماكرو أشد وأكبر من خطر الفيروسات التقليدية.

٣- هذا النوع من الفيروسات لا يتقيد بنظام تشغيل معين، فهناك مثلاً إصدارات من برنامج Word الشهير لأنظمة Windows باختلاف أنواعها، مما يجعل إمكانية الإصابة بهذا النوع من الفيروسات أكبر.

وليست فيروسات الماكرو حكراً على برنامج Word، فهناك فيروسات تصيب برنامج Word Pro من Lotus ولكنها لا تكون متعلقة بالوثيقة كما هي الحال في برنامج "Word" وإنما في ملف منفصل.

وهناك أنواع أخرى كثيرة من الفيروسات التي تصيب نوعاً معيناً من الملفات حسب أسمائها أو أنواعها ويضيق المجال هنا عن ذكرها وخاصة أن انتشارها بات محدوداً جداً.

٤.١٢ فيروسات البريد الالكتروني :

هذا النوع من الفيروسات ينتقل عبر الملفات المرفقة مع البريد الالكتروني وباستخدام برنامج حماية من الفيروسات محدث وبتوخي الحذر عند فتح مرفقات ملفات وبالنقر فوق ارتباطات في رسائل، ينبغي تجنب إصابة الكمبيوتر بـ فيروس من بريد-إلكتروني ضار.

فاتبع هذه الإرشادات لحماية الكمبيوتر:

توخي الحذر في حالة فتح مرفقات البريد-الإلكتروني

تعتبر مرفقات البريد-الإلكتروني مصدرًا أوليًا للإصابة بالفيروس. على سبيل المثال، يمكن تلقي بريد-إلكتروني، حتى من شخص ما تعرفه، به ملف مرفق متخفي على شكل أحد المستندات أو الصور أو البرامج، لكنه بالفعل فيروس. وفي حالة فتح ذلك الملف، سيصيب الفيروس الكمبيوتر. وما يعتبر خبرًا جيدًا هو أن بريد Windows يمنع تلقائيًا أنواع الملفات الخطيرة المعروفة. ومع ذلك، يجد صانعوا الفيروسات تقنيات

جديدة لنشر برامجهم الضارة، لذلك ينبغي توخي الحذر في حالة فتح المرفقات. وفي حالة تلقي مرفقات بريد-إلكتروني لم تكن متوقعة، عليك الاهتمام بالرد على مرسليها ومطالبتهم بالتحقق من أنهم بالفعل أرسلوا المرفقات قبل أن تفتحها.

✓

استخدام برنامج حماية من الفيروسات لفحص محتويات الملفات المضغوطة

يعتبر الأسلوب الوحيد الذي يستخدمه صانعوا الفيروسات لجعل الملفات الضارة تتسلل إلى الكمبيوتر هو إرسالها كمرفقات باستخدام تنسيقات الملفات المضغوطة، مثل .zip و .rar وستفحص معظم برامج الحماية من الفيروسات هذه المرفقات لأنه قد تم تلقيها، ولكن حتى تكون في أمان، ينبغي حفظ المرفقات المضغوطة في أحد المجلدات على الكمبيوتر واستخدام برنامج الحماية من الفيروسات لفحصها قبل فتح أية ملفات متضمنة فيه.

✓

توخي الحذر أثناء النقر فوق الارتباطات في الرسائل

يتم غالبًا استخدام رسائل خادعة في رسائل البريد-الإلكتروني كجزء من محاولات الخداع والتجسس، ولكن يمكن استخدامها أيضًا لإرسال الفيروسات. وقد ينقلك النقر فوق ارتباط خادع إلى صفحة ويب تحاول تنزيل برامج ضارة إلى الكمبيوتر. فيجب توخي الحذر في حالة تقرير النقر فوق أحد الارتباطات من عدمه، وخاصة إذا كان نص الرسالة يبدو غامضًا وغير محدد، مثل قراءة الرسالة "التحقق من صور الإجازة" دون وجود أية معلومات تحددك أو تحدد المرسل بشكل خاص.

٥ - أعراض الإصابة بالفيروس :

تصاحب الأعراض التالية ظهور الفيروس وتعتبر علامات الإصابة به :

٥.١ - نقص شديد في الذاكرة للذاكرة ثلاث حالات.. فقبل دخول الفيروس تكون الذاكرة في حالة طبيعية. ثم بعد أن يبدأ الفيروس في العمل يلاحظ نقص شديد في الذاكرة. وذلك لأن الفيروس في هذه الحالة يبدأ في تدمير الذاكرة وكذلك ملفات التبادل Swap Files عن طريق إزالة البيانات المخزنة، مما ينتج عنه توقف البرنامج العامل في الوقت ذاته لعدم وجود أي بيانات في الذاكرة، وإنما يستبدلها الفيروس بمجموعة من الأصفار في مكان تعليمات التشغيل. أما الحالة الثالثة بعد أن يكرر الفيروس نفسه يحتل الذاكرة.

٥.٢- الخطأ في استخدام لوحة المفاتيح عن طريق إظهار أحرف غريبة أو خاطئة عند النقر على حرف معين.

٥.٣- استخدام القرص الصلب بطريقة عشوائية. وتستطيع أن تلاحظ ذلك من إضاءة لمبة القرص الصلب حتى وإن كان لا يعمل.

٥.٤- تغيير في عدد ومكان الملفات وكذلك حجمها بدون أي أسباب منطقية.

٥.٥- بطء تشغيل النظام بصورة مبالغ فيها.

٥.٦- عرض رسائل الخطأ بدون أسباب حقيقية.

٥.٧- توقف النظام بلا سبب.

٥.٨- إختلاط أدلة القرص أو رفض النظام العمل منذ البداية

٦- إستراتيجية الهجوم للفيروس :

أهداف هامة يجب عليه أن ينجزها وهي إما أن تكون برنامجاً أو ملفاً معيناً. وهدف الهجوم يختلف من فيروس إلي آخر وأيضاً حسب نظام التشغيل.

٦.١- أماكن الفيروس الإستقرارية :

يبحث الفيروس عن أهداف يضمن وجودها في أي نظام تشغيل وهي التي لا يستطيع أي نظام أن يعمل بدونها. وفي نظام Windows أو أي إصدار من أي نظام تشغيل آخر يعتمد على DOS فإن الملف المستهدف دائماً من قبل الفيروسات هو COMMAND.COM.

وذلك لأن الملف موجود دائماً في الدليل الرئيسي للفهرس الخاص بالنظام حيث أن هذا الملف هو المسؤول عن استقبال أوامر التشغيل التي تدخلها وتقرير تنفيذها إن كانت من أوامر التشغيل الداخلية أو من أوامر التشغيل الأخرى التي تنتهي بالامتدادات COM, EXE, BAT . وفيروسات هذا النوع أكثر تنوعاً من فيروسات قطاع بدء التشغيل.

٧ـ تصنيفات الفيروسات :

٧,١ـ الفيروسات المتطفلة :

وهي التي تلصق نفسها بالملفات لكي تتكاثر وتبقي الملف الأصلي بحالة سليمة في الغالب.

٧.٢- الفيروسات المرافقة :

تعتمد على قاعدة الأسبقية في التنفيذ للملفات COM. وتتمكن من نقل العدوى عن طريق إنشاء ملف جديد بدون تغيير طول الملف.

٧.٣- الفيروسات الرابطة:

تصيب البرامج بتغيير المعلومات في جدول مواقع الملفات FAT بحيث تبدأ البرامج المصابة من الموقع ذاته، وهو عادة الـ Cluster الأخير في القرص والذى يتضمن نص الفيروس، مما يضمن له انتشاراً سريعاً كما في فيروس DIRII.

٧.٤- الفيروسات المستبدلة:

تقوم بالكتابة فوق جزء من البرنامج بدون تغيير حجم الملف، مما يؤدي إلي فشل البرنامج عند تنفيذه كما في فيروس BURGER405. وهناك حيلة يلجأ إليها بعض المبرمجين الأذكياء. بتغيير إسم هذا الملف لكي يصعب على الفيروس ربط نفسه به. وهناك أيضاً ملفات YS, CONFIG, BAT, AUTOEXEC حيث يبحث النظام عنها عند بدء التشغيل وينفذ ما بها من تعليمات. وهناك ملفات أخرى تمثل إغراء أكثر جاذبية للفيروس وهي: IBMBIO.COM, IBMDOS.COM لأنها ملفات مخفية فبالرغم من وجودها في الفهرس الرئيسي إلا إنه يصعب اكتشاف الفيروس عند عرض دليل الملفات. ومن أماكن الفيروسات المفضلة مخزن COMS. وهو مكان في الذاكرة يتم عن طريقه ضبط ساعة النظام.

وهذا المكان في منتهى الخطورة لأنه:

- توجد به طاقة عن طريق البطاريات التي تستخدم في المحافظة على توقيت النظام حتى بعد أن يتم إغلاق الكمبيوتر.
- لأنها أول مكان يتم تشغيله عند بدء التشغيل. كما أن هذا المكان لا يظهر عند عرض الملفات بالأمر DIR.
- عن طريق هذا المكان يحدد الفيروس توقيت تشغيله متى حانت ساعة الصفر. المكان الآخر الذي يمكن للفيروسات إصابته والاستقرار فيه

هو ملفات البرامج وخاصة الملفات التنفيذية من نوع COM. و EXE. أو SYS. وغيرها .

٨- أشكال الفيروسات :

تظهر الفيروسات في عالم الكمبيوتر بأشكال عديدة أهمها:

٨.١- السريع :

بمجرد دخول هذا النوع من الفيروسات إلي الكمبيوتر يصيب كل الملفات التي يتم تنفيذها في ذلك الوقت، وهي ليست خطيرة كثيراً كما يمكن أن يتخيل البعض، فالتخلص منها سهل للغاية، حيث تقوم معظم برامج حماية الفيروسات بفحص الذاكرة الرئيسة بشكل دوري، ومن الطبيعي أن يكون الفيروس السريع متواجداً هناك، إذ يصيب كل الملفات الموجودة في الذاكرة، عندها يتم اكتشافه من قبل برنامج الحماية فإنه يتخلص منه.

٨.٢- البطيء :

تتلخص فكرة هذا النوع من الفيروسات أنه كلما كان انتشاره بطيئاً صعب اكتشافه والتخلص منه سريعاً. وهناك العديد من الطرق التي يمكن أن يعمل بها، ولكن الأسلوب التقليدي الذي يعمل به الفيروس البطيء هو إصابة الملفات التي كنت تنوي تعديلها، مما يعني إنه لو كنت تشغل كاشف للتغييرات كحماية ضد الفيروسات، يخبرك عندها أن هناك إصابة وتغيير في أحد الملفات، ولكن بما أنك قررت عمل تغييرات

في ذلك الملف أصلاً فستوافق على ذلك، وتتقبل الفيروس. وعندما تنسخ ملفاً على قرص مرن، يكون ذلك الملف معطوباً أصلاً، وعند نسخه على كمبيوتر آخر محمي ببرامج الحماية ضد الفيروسات وبكاشف التغييرات على الملفات الذي يحذرك من التغيير الذي طرأ على الملف الأصلي فتؤكد له معرفتك بذلك ظاناً أنه يعطيك تحذيراً على التغييرات التي قمت أنت بها، وتكون النتيجة إصابة الكمبيوتر الثاني بالفيروس.

٨.٣- المتسلل :

هو ذلك الفيروس الذي يختبئ في الذاكرة الرئيسية ويسيطر على المقاطعات. يكون لكل جهاز طرفي رقم معين من قبل المعالج الرئيسي يسمى مقاطع، مهمته تنسيق التخاطب بين الأجهزة الطرفية المختلفة داخل الكمبيوتر. ففي حالة الفيروس الذي يصيب مقطع التشغيل فإنه يسيطر على مقاطع القراءة/ الكتابة على القرص الصلب رقم ١٣h، وإن كان متسللاً فإن أي برنامج يحاول القراءة من مقطع التشغيل يقوم الفيروس بقراءة المعلومات الأصلية التي قام بتخزينها في مكان آخر بدلاً من المعلومات المعطوبة في مقطع التشغيل، ولا يشعر المستخدم بأي تغيير ولا يتمكن من لمس الفرق.

٨.٤- متعدد الأشكال :

تعتبر برامج حماية الفيروسات التي تستخدم تقنية مسح الذاكرة بحثاً عن الفيروسات هي الأكثر شيوعاً في العالم، لذلك تكون هذه البرامج

هي التحدي لكل مبرمج للفيروسات يحاول التغلب عليه. لذا وجدت الفيروسات متعددة الأشكال، التي لو تمت مقارنة نسختين من الفيروس نفسه معاً لم تتطابقا. وهذا يصعب مهمة برامج الحماية ويتطلب منها القيام بأمور مختلفة أكثر تعقيداً لاكتشاف هذا النوع من الفيروسات.

٩- المشاكل التي يسببها الفيروس :

٩.١- تباطؤ أداء الكمبيوتر، أو حدوث أخطاء غير معتادة عند تنفيذ البرنامج .

٩.٢- زيادة حجم الملفات، أو زيادة زمن تحميلها إلي الذاكرة .

٩.٣- سماع نغمات موسيقية غير مألوفة .

٩.٤- ظهور رسائل أو تأثيرات غريبة على الشاشة .

٩.٥- زيادة في زمن قراءة القرص إذا كان محمياً وكذلك ظهور رسالة FATALI/O ERROR.

٩.٦- تغيير في تاريخ تسجيل الملفات كما في فيروس Vienna الذي يكتب ٦٢ مكان الثواني.

٩.٧- حدوث خلل في أداء لوحة المفاتيح كأن تظهر رموز مختلفة عن المفاتيح التي تم ضغطها كما في فيروس Haloechon أو حدوث غلق للوحة المفاتيح كما في فيروس. Edv.

٩.٨- نقص في مساحة الذاكرة المتوفرة كما في فيروس Ripper الذي

يحتل ٢ كيلو بايت من أعلى الذاكرة الرئيسية. ويمكن كشف ذلك بواسطة الأمر MEM أوCHKDSK.

٩.٩- ظهور رسالة ذاكرة غير كافية لتحميل برنامج كأن يعمل سابقاً بشكل عادي.

٩.١٠- ظهور مساحات صغيرة على القرص كمناطق سيئة لا تصلح للتخزين كما في فيروس Italan وفيروس Ping Pong اللذين يشكلان قطاعات غير صالحة للتخزين مساحاتها كيلوبايت واحد.

٩.١١- عطيل النظام بتخريب قطاع الإقلاع SECTOR BOOT.

٩.١٢- إتلاف ملفات البيانات مثل ملفات Word و Excel وغيرها.

١٠- الوقاية من الإصابة بالفيروسات :

- فحص جميع الأقراص الغريبة أو التي استخدمت في أجهزة أخرى قبل استخدامها.

- تهيئة جميع الأقراص اللينة المراد استخدامها على جهازك.

- عدم تنفيذ أي برنامج مأخوذ من الشبكات العامة مثل الإنترنت قبل فحصه.

- عدم إقلاع الكمبيوتر من أي قرص لين قبل التأكد من خلوه من الفيروسات.

- عدم ترك الأقراص اللينة في السواقة عندما يكون الجهاز متوقفاً عن العمل.

- التأكد من خلو سواقة الأقراص اللينة قبل إعادة إقلاع الجهاز.

- عدم تشغيل برامج الألعاب على الجهاز ذاته الذي يتضمن البيانات والبرامج الهامة.

- حماية الأقراص اللينة ضد الكتابة لمنع الفيروسات من الانتقال إليها.

- استخدام برامج أصلية أو مرخصة.

- استخدام كلمة سر لمنع الآخرين من العبث بالكمبيوتر في غيابك.

- الاحتفاظ بنسخ احتياطية متعددة من جميع ملفاتك قبل تجريب البرامج الجديدة.

- تجهيز الكمبيوتر ببرنامج مضاد للفيروسات واستخدامه بشكل دوري.

- تحديث البرامج المضاد للفيروسات بشكل دائم لضمان كشف الفيروسات الجديدة.

- استخدام عدة برامج مضادة للفيروسات ومختلفة في طريقة البحث عنها في الوقت ذاته.

- الاحتفاظ بنسخة DOS نظيفة من الفيروسات ومحمية ضد الكتابة لاستخدامها عند الإصابة.

- الانتباه للأقراص اللينة الواردة من المعاهد والكليات الأماكن التقليدية للفيروسات.

- إغلاق الجهاز نهائياً وإعادة تشغيله عند ظهور عبارة Non Bootable Diskette.

١١- محركات البحث على الإنترنت قد تنقل الفيروسات وتكشف الاسرار:

نشر في مجلة New Scientist في عددها الصادر في نوفمبر ٢٠٠١ أن محركات البحث الجديدة مثل www.google.com من الممكن أن تسمح للمخترقين الهاكر باكتشاف الأرقام السرية وأرقام بطاقات الائتمان وكذلك المساعدة في نشر الفيروسات عبر الإنترنت. حيث تستخدم محركات البحث الجديدة نظام بحث يعمل من خلال مسح ملفات مخبأة عن محركات البحث القديمة التي تبحث من خلال صفحات الويب المكتوبة بلغة الـ HTML . وحذر خبراء في هذا المجال من أن طريقة عمل محركات البحث مثل Google قد توفر وسيلة سهلة للإختراق وكشف أسرار قواعد البيانات غير المحمية. ويجدر القول بأن الملفات من نوع Word أو Acrobat يتم فحصها من الفيروسات بواسطة محرك البحث Google أما الملفات من النوع Lotus 1-2-3 أو MacWrite أو Excel أو PowerPoint أو Rich Text Format فمن المحتمل أن تحتوي على أرقام سرية

وأرقام بطاقات الائتمان التي تعتبر أحرف يمكن لمحرك البحث بالبحث عنها في تلك الملفات.

١٢ - طرق انتشار الفيروسات :

يمكن أن ينتقل الفيروس من حاسوب مصاب إلى حاسوب سليم عن طريق نسخ الأقراص المرنة أو عبر خطوط الاتصالات أو ضمن الشبكات ويمكن تمييز نوعين من عدوة الفيروسات:

١_ عدوة مباشرة:

عندما يتم تنفيذ برنامج مصاب بفيروس فإن الفيروس يبحث بنشاط عن ملف أو أكثر لينقل إليه العدوى وهذا النوع قليل الانتشار لأن آلية العدوى ليست فعَالة كثيراً

٢_ عدوة غير مباشرة:

عندما يتم تشغيل برنامج مصاب فإن الفيروس ينتقل إلى ذاكرة الحاسوب ويستقر فيها ويتم تنفي البرنامج بشكل بيعي ولكن عند تحميل أي برنامج آخر إلى الذاكرة يتم انتقال العدوى إلى ذلك البرنامج وتتكرر العملية إلى أن يتم قطع التغذية الكهربائية عن الحاسوب أو عند إعادة تشغيله

ملاحظة: إن ما تستطيع فيروسات الحاسوب عمله عندما يتم تنشيها يعود إلى خبرة مبرمجها ومعرفته العلمية لذلك فبعضها يصدر نغمة موسيقية أو يظهر رسالة على الشاشة.

إن أشد الفيروسات ضرراً وأكثرها خطورة هي التي تسبب الضرر في الخفاء دون أن تسمح لك بمعرفة ما يحدث وعندما يتم كشفها يشكل تأثيرها الضار كارثة كبيرة مثل فيروس DATD CRIME

١٣ – صيانة جهاز مصاب بالفيروسات :

عندما يصيب الفيروس الحاسب ، فإن أول ما يجب القيام به هو استخدام أحد برامج مضادات الفيروسات و التي يتم تحديثها باستخدام شبكة المعلومات بشكل دوي حتى تستطيع التعرف علي أحدث أنواع الفيروسات ، و في حالة الشك بأن أحد الملفات مصاب بفيروس معين ولكن البرنامج المضاد للفيروسات لا يستطيع التعرف علية فيمكن إرسال هذا الملف إلى الشركة المنتجة للبرنامج المضاد للفيروسات حتى يتم الكشف عليه ، وفي حالة الإصابة الفعلية لها الملف تقوم الشركة بإرسال مضاد لهذا الفيروس حتى يستطيع المستخدم القضاء علي الفيروس ، و من برامج مضادات الفيروسات التي يوجد بها هذه الإمكانية برنامج Norton Anti Virus ، و للأسف الشديد لا يوجد الكثير مما يمكن أن يقوم به المستخدم في حالة إكتشاف وجود الفيروس بخلاف إستخدام مضادات الفيروسات ، و لذلك فإن وجود نسخ احتياطية من الملفات المهمة يعد أمر ضروري ، ويفضل أن يتم عمل هذه النسخ علي أقراص مدمجة و ليس أقراص مرنة لضمان

سلامتها و عدم تعرضها للتلف السريع ، ومن طرق حماية وصيانة الحاسب المصاب بالفيروسات هي :

اولا : المسح ضد الفيروسات : Virus Scanning :

تستطيع أن تقوم بعملية مسح فورية مجانية لكمبيوترك الشخصي ضد الفيروسات من الموقع التالي /www.centralcommand.com اضغط على الوصلة Free Online Virus Scan لتنتقل إلى صفحة جديدة، حيث تقوم بإدخال البيانات الشخصية وبعدها تبدأ عملية الفحص الفوري لجهازك.

ثانيا: تحميل برنامج مقاوم للفيروسات:

الخطوة السابقة المتمثلة في فحص الكمبيوتر فورا عبر الإنترنت، شيء ضروري ومهم، ولكنه لا يغنيك عن تنزيل وتحميل برنامج مقاوم للفيروسات. مثل البرنامج الممتاز AVG الذي تستطيع استدعاءه من الموقع التالي

www.grisoft.com/html/us_downl.htmlوهو برنامج مجاني يقوم بترقية نفسه بنفسه، حسب إعدادك له.

ثالثا: تصفية Filtering مرفقات البريد الإلكتروني:

كما يصفي أحدنا الماء من الشوائب، فانه يستطيع تصفية مرفقات البريد الإلكتروني من الفيروسات. الطريقة المثلى لذلك، هو أن يضع قواعد للبريد الإلكتروني الوارد، بحيث تتوجه الرسائل الواردة

مباشرة الى مجلد خاص لتفحصها هناك٠ تتم هذه العملية في أوت لوك اكسبريس على النحو التالي، اختر Tools Message Rules Mailفتظهر النافذة الخاصة بإعداد القواعد الخاصة بالبريد الإلكتروني٠

رابعا: راقب امتدادات Extensions الملفات المرفقة:

تستطيع أن ترصد فيروسا داخل ملف مرفق، إذا دققت في اسم الملف٠ فإذا كان منتهيا بالامتداد VBS٠ فانه سيكون مثار شك وريبة، لأن هذا الاسم لن يكون لملف نصي بالهيئة وورد، وإنما ملف فيجوال بيسك سكريبت الذي قد يحتوي على فيروس ٠

خامسا: الماكرو فيروس : Macro Virus

لسوء الحظ أن مستندات وورد قد تحتوي على فيروسات مختبئة٠ فاذا كنت تستخدم وورد ٢٠٠٠ فقد تحمي نفسك نسبيا إذا رفعت مؤشر الأمان على النحو التالي، اختر Tools Macro Security ومن النافـــذة الجديدة تأكد بأن المؤشر مرفوع للأعلىHigh

سادسا: وقايـة كتــاب العنــاويــن:

Address Book في أوت لو اكسبريس ٦ تســتطيع أن توقـــف الفيروســـات، عن نســخ نفسـها وإرسـال هـذه النسخ إلى عناويـــن البريد الالكترونيـــة الموجــودة في كتاب العناوين، وذلك على النحو التالي، اختر Tools Options ثم

اختـر التبويبة Security وضـــع علامة الصـح في المربع

الصغــير بجانـب العبـارة Warn me when other applications try to send mail as me

سابعا: خدمة فورية للقضاء على الفيروسات الخطيرة:

إذا شككت بأن كمبيوترك أصيب بفيروس خطير مثل الفيروس

نيمدا على سبيل المثال، فاذهب إلى الموقع التالي:

www.centralcommand.com/jan1.html تجد قائمة

بأخطر ١٢ فيروسا ودودة كمبيوترية، ومن الموقع تحصل على رزمات

برمجية للقضاء عليها.

ثامنا :فحص الأقراص المرنة التي استخدمت في حاسوب آخر قبل

تشغيلها في حاسوبك

تاسعا : إعادة تهيئة جميع الأقراص المرنة المصابة المراد استخدامها

على حاسوبك

عاشرا _عدم تنفيذ أي برنامج تم تحميله من شبكات الانترنت

internet قبل التأكد من خلوه من الفيروسات

الحادي عشر: عدم تشغيل برامج الألعاب على الجهاز الذي

يتضمن معلومات وبيانات هامة

الثاني عشر: استخدم برامج أصلية أو مرخصة لشركات معروفة

الثالث عشر: تجهيز الحاسوب ببرنامج مضاد للفيروس واستخدامه

بشكل دوري أو تحديث هذا البرنامج لضمان كشف الفيروسات الجديدة والقضاء عليها

شرح المصطلحات الواردة في الموضوع:

١. **كتاب العناوين** Address Book :

هو بمثابة سجل يحتوي على عناوين البريد الإلكترونية لأصدقاء أو معارف، بحيث يمكن الرجوع اليه كلما أردت عنوان أحد منهم.

٢. **التروجان** Trojan **أي طروادة:**

وهو الحصان الذي تخفى فيه المهاجمون لدخول القلعة والفتك بأهلها، عبارة عن فيروس متخف في برنامج أو ملف، وهو أخطر أنواع الفيروسات، لأنه يفتك بالكمبيوتر، ولكنه لا ينسخ نفسه ويرسلها إلى كتاب العناوين.

٣. مؤشر الأمن Security Level :

عبارة عن رافعه كلما حركتها للأعلى ازدادت مستويات الأمن والسرية، والوقاية من الفيروسات

الرابع عشر: البرامج المضادة للفيروسات:

لقد تنوعت برامج تفحص الفيروسات في الآونة الأخيرة وهي تؤدي عملاً متشابهاً يتجلى ي حماية الحاسوب من فيروسات دخيلة عليه عن طريق أقرا التخزين المرنة أو الليزرية أو من خلال فتح الانترنت وتصفح المواقع

من هذه البرامج :

Norton Antivirus ,Kspersky Antivirus, MaccAfee Antivirus

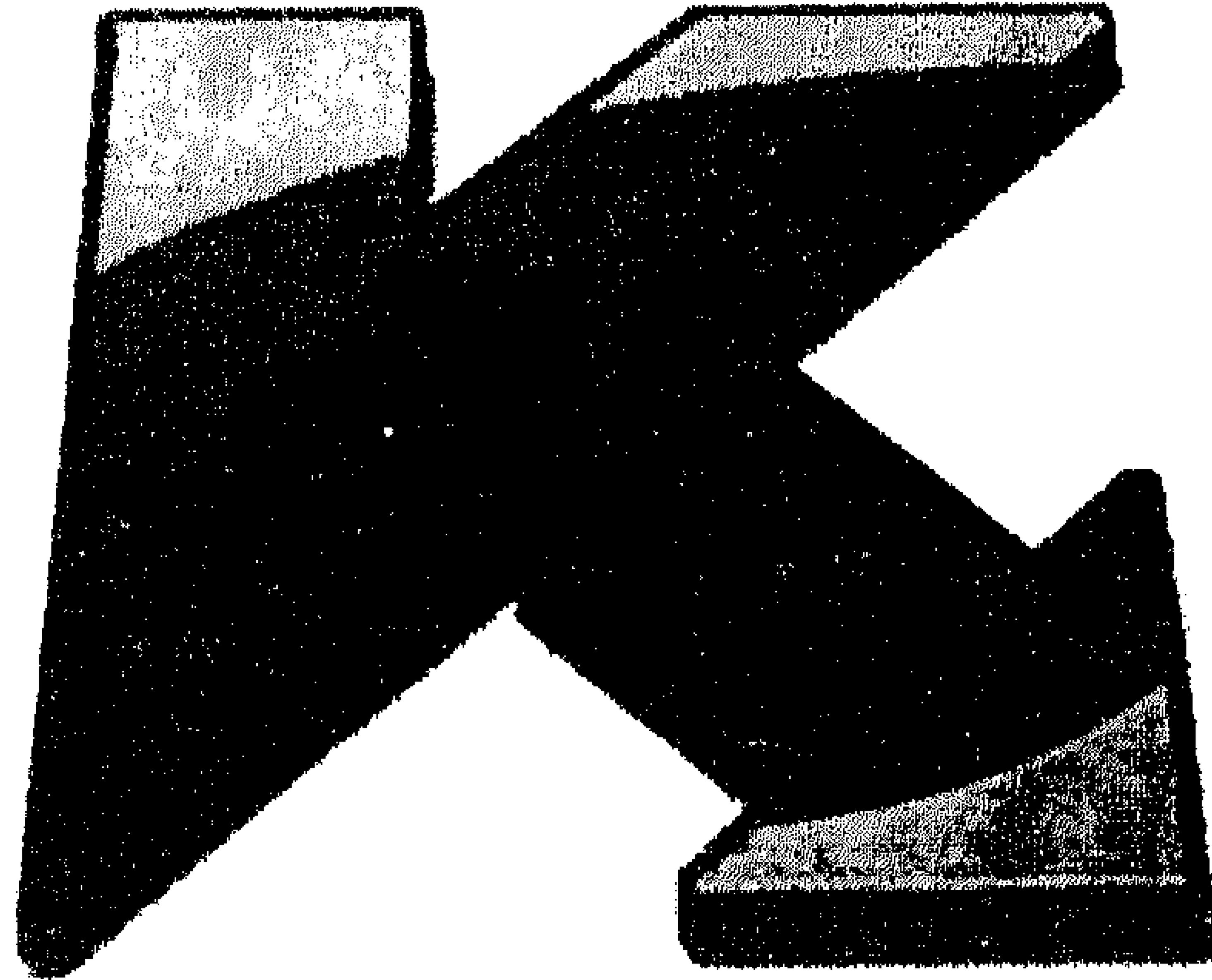
يمكن تحميل أحد هذه البرامج على القرص الصلب إما من برنامج موجود على قرص ليزري أو من خلال الانترنت.وأثناء التحميل تظهر رسالة تتيح لنا إمكانية جعل هذا البرنامج يعمل أثناء إقلاع الحاسوب وبعد التحميل يظهر رمز خاص بالبرنامج ضمن شريط المهام يمكن فتح البرنامج من خلال النقر على رمز أيقونته نقرا مزدوجا وعندما نريد فحص مجلد ما للتأكد من خلو ملفاته من فيروسات ننقر على المجلد المطلوب بالزر الأيمن للماوس ونختار scan with Norton Antivirus ويظهر مربع يبين نتيجة تفحص من الفيروسات وتتضمن عدد الملفات التي تم حذفها.........

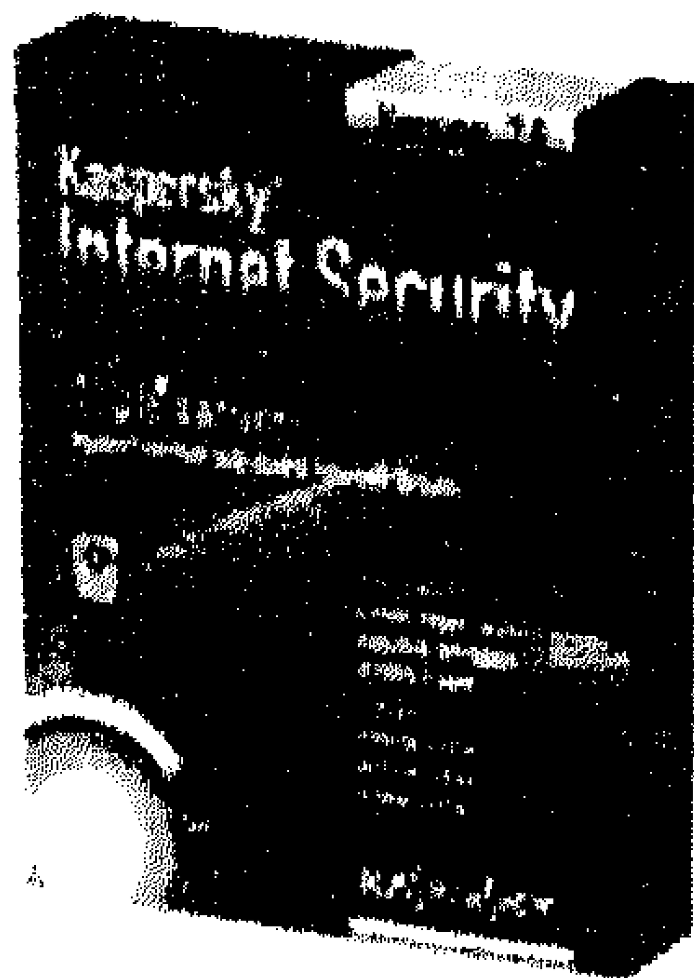
في هذه الحالة لم يعثر البرنامج على الفيروسات ولكن أحتوى المجلد عل فيروسات سوف تظهر نافذة تبين مكان توضع الفيروس واسمه حيث

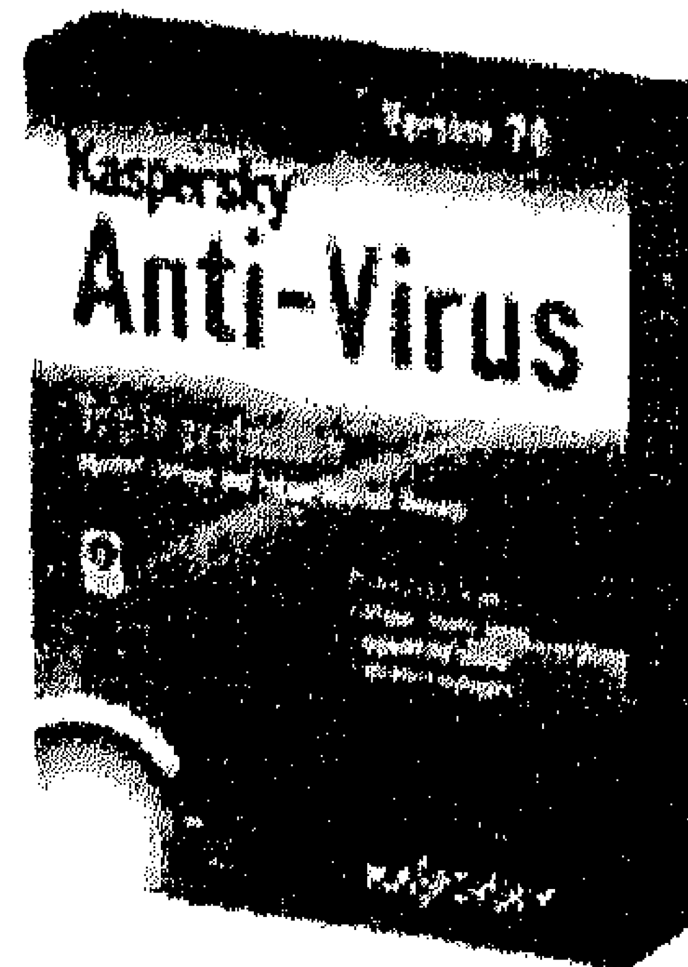
قام البرنامج بحذفه بشكل آلي وعند النقر على ok تأكيداً لموافقتنا تظهر نافذة تبين الانتهاء من حذف الفيروس .

١٥ - تثبيت وتهيئة البرامج المضادة للفيروسات :

تعلم تنصيب الكاسبر سكاي انترنيت سكيورتي v.8







Kaspersky Internet Security 2009

Kaspersky Anti-Virus 2009

8.0.0.357 - *Final*

English - French - Arabic

معلومات عن البرنامجين

برنامج Kaspersky برنامج كاسبر ٨ بكل تاكيد تعرف هذا العملاق من روسيا ؟ نعم

* أنه العملاق الروسي هذا العملاق الذي تفوق على اقوى منافسين وتحدى شركات عملاقة وتخطاها خلال زمن قصير جداً عندما تقوم بتحميل هذا

* البرنامج وتنصيبه في حاسوبك سوف يجعلك مطمئن وانتا تتصفح المواقع ومشاركة

* ملفاتك واستقبال ايملات يقوم بتحديث كل ثانية نعم كل دقيقة وثانية ضد

* الفيروسات وملفات التجسس ... ريح بالك واقضي واسحق كل الفيروسات وملفات التجسس بواسطة عملاق المكافحة الروسي

كاسبر

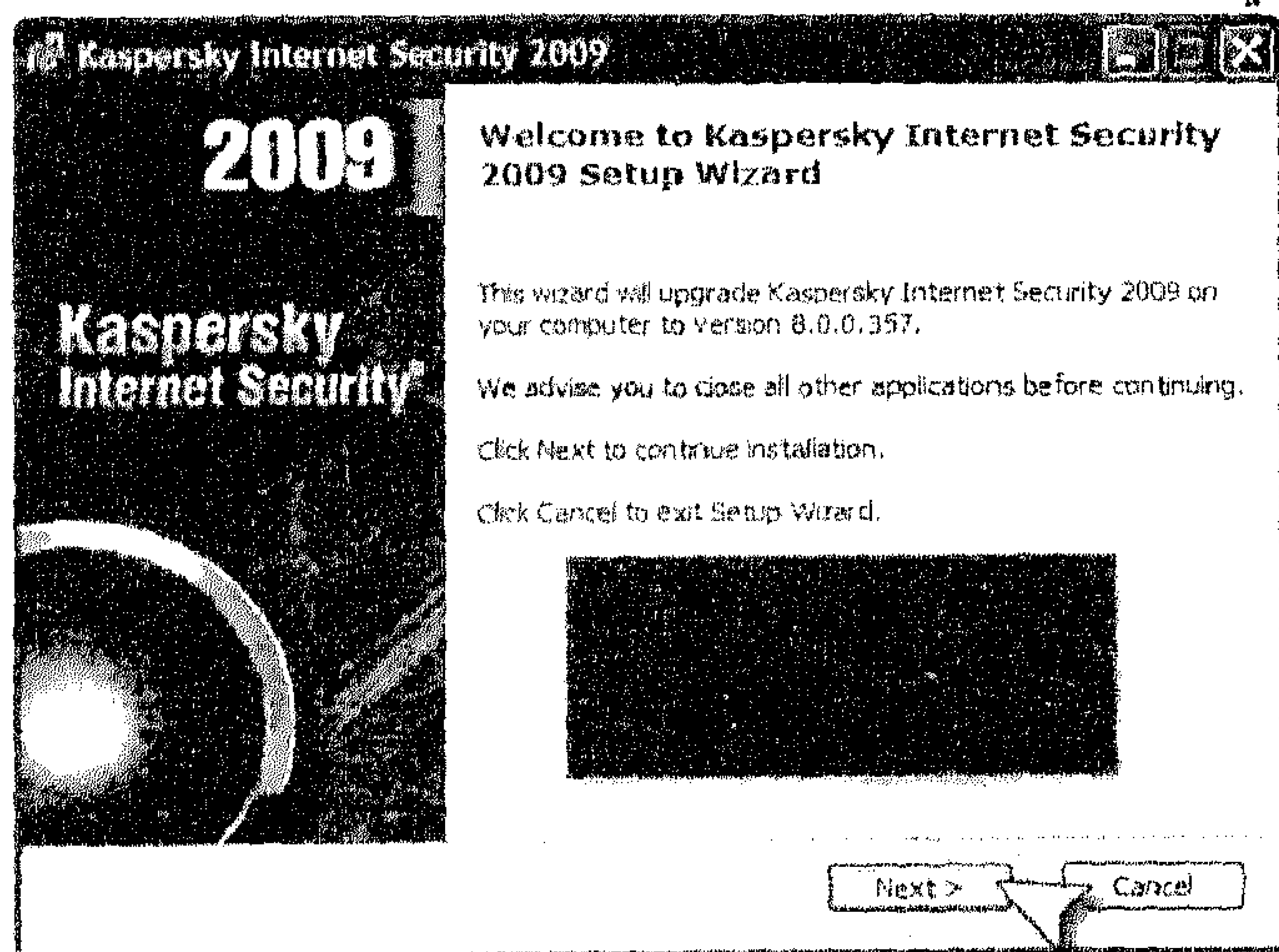
* برنامج رائع قوي لحماية الجهاز من المخترقين ، فهو بإفضافة الى كونه جدار حماية فهو يحتوي على مضاد للفيروسات و مضاد لرسائل المزعجة او التي تحتوي على فيروسات والعديد من المهام مهما كتبت سوف لن استطيع أن اعطي هذا العملاق حقه لن أطيل عليكم فهذا الرآئع لا يحتاج لوصف .

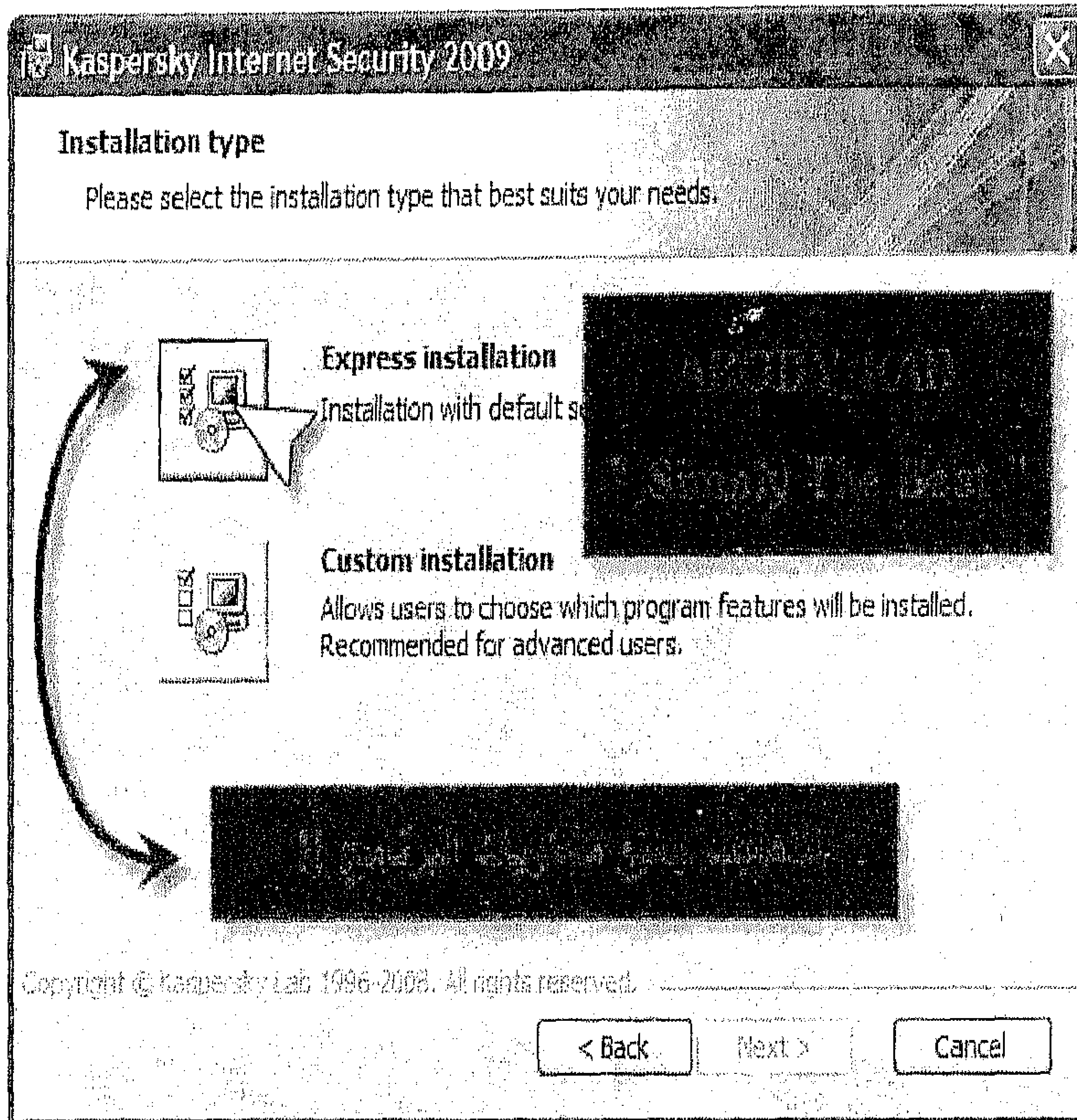
تنصيب البرنامج

أنا قمت بتنصيب الإنترنت سكيوتري فقط!

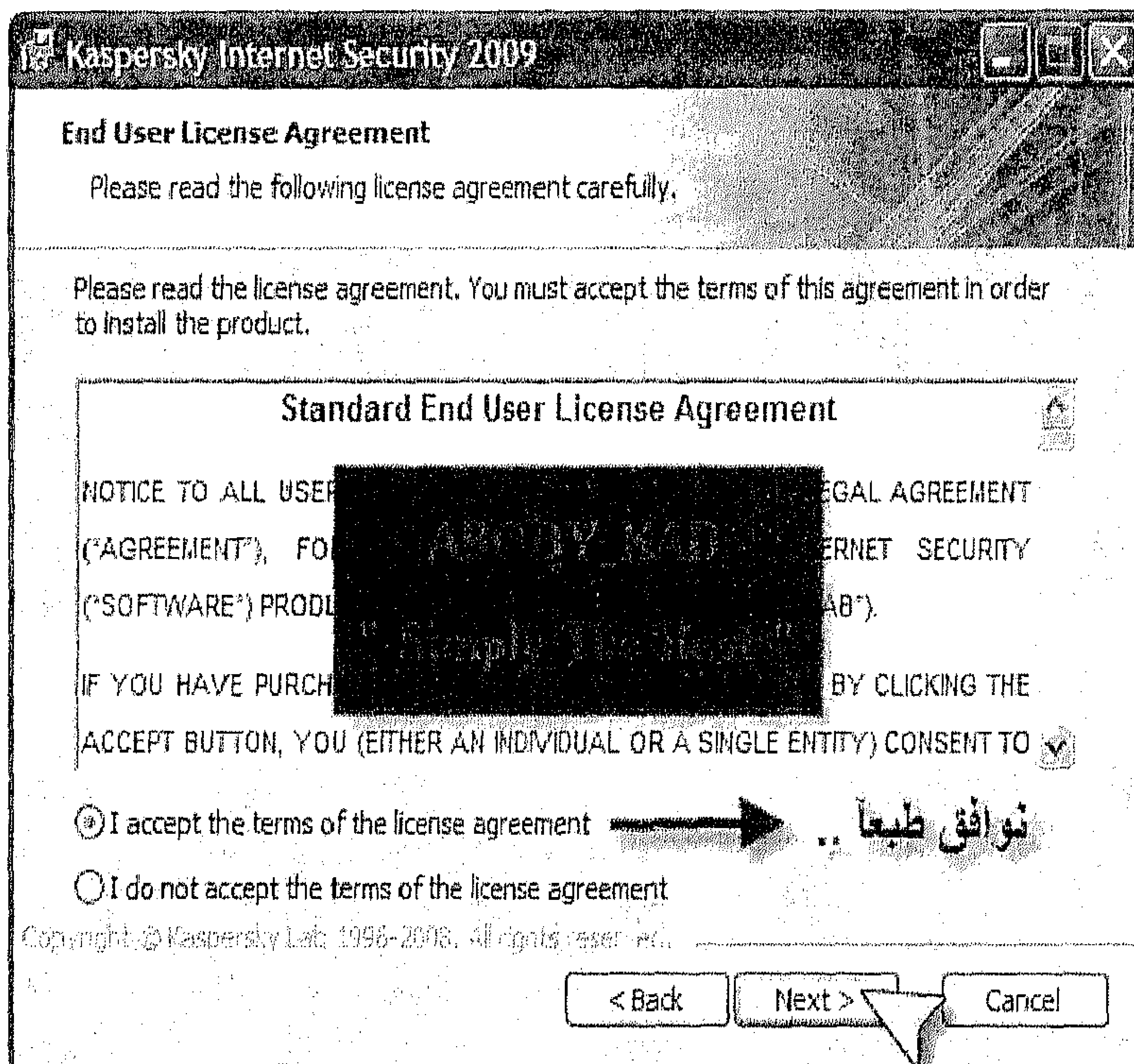
و الأنتي فايروس لا يفرق عنه أبدآ!

خطأ

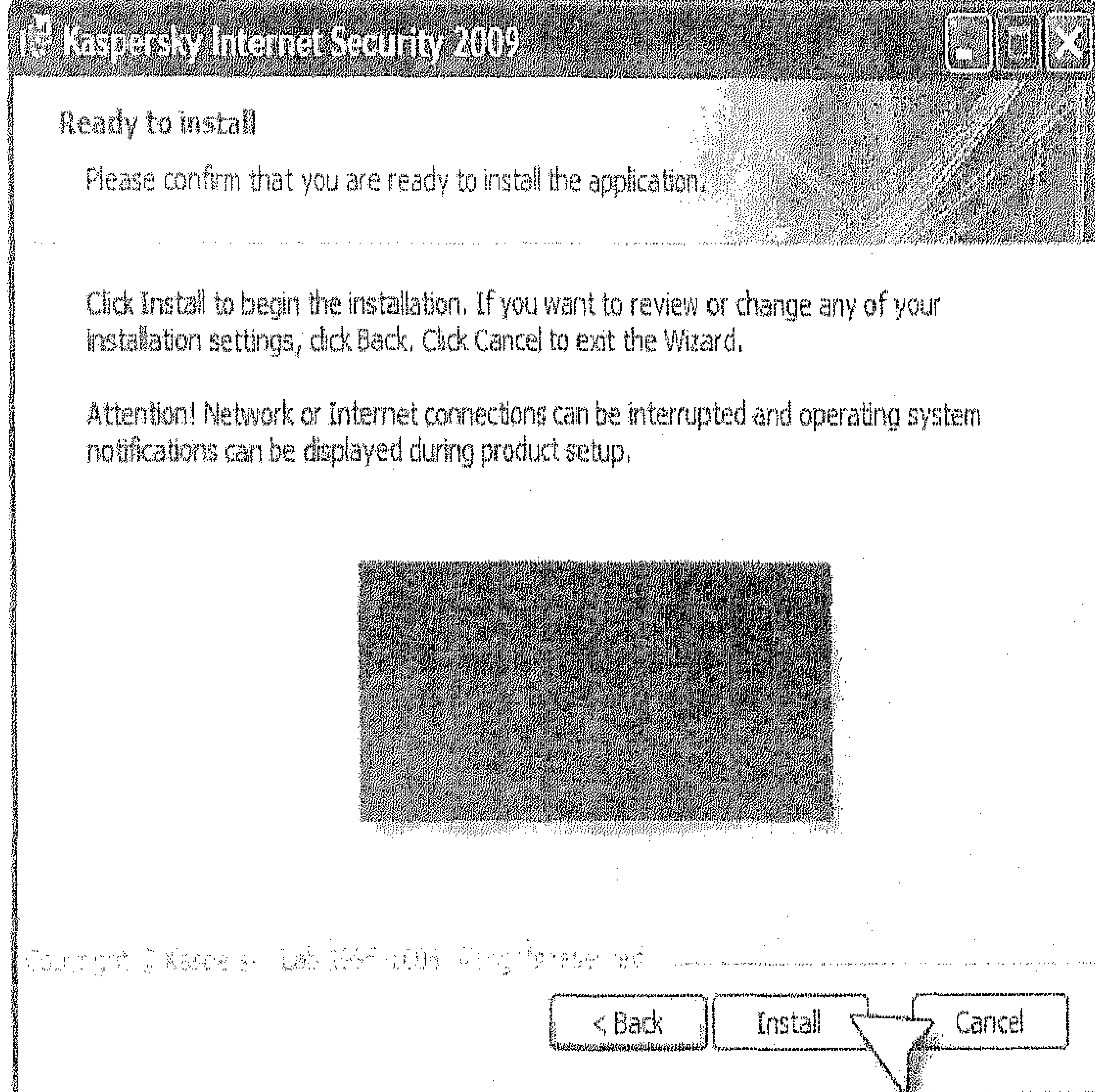


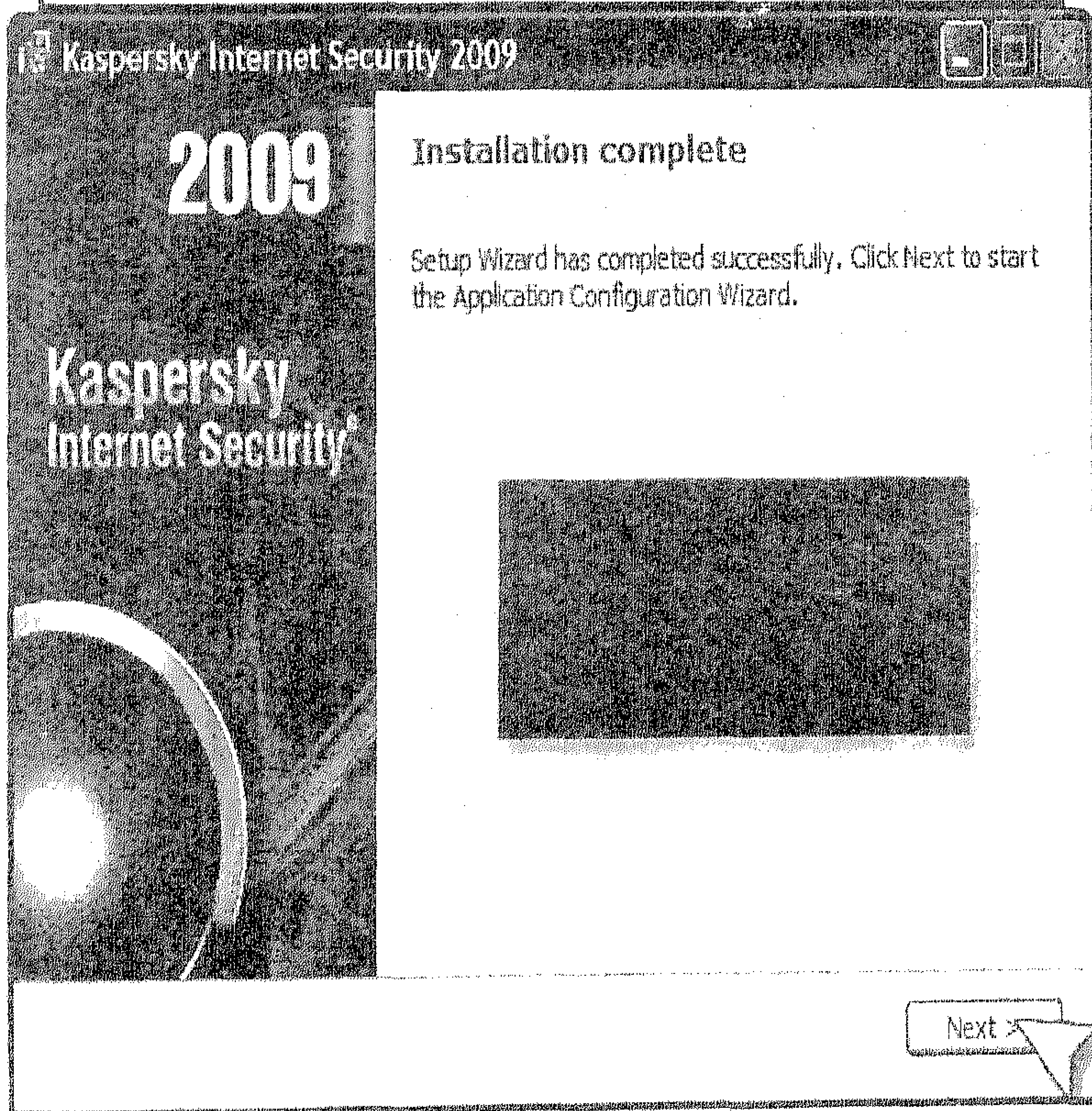


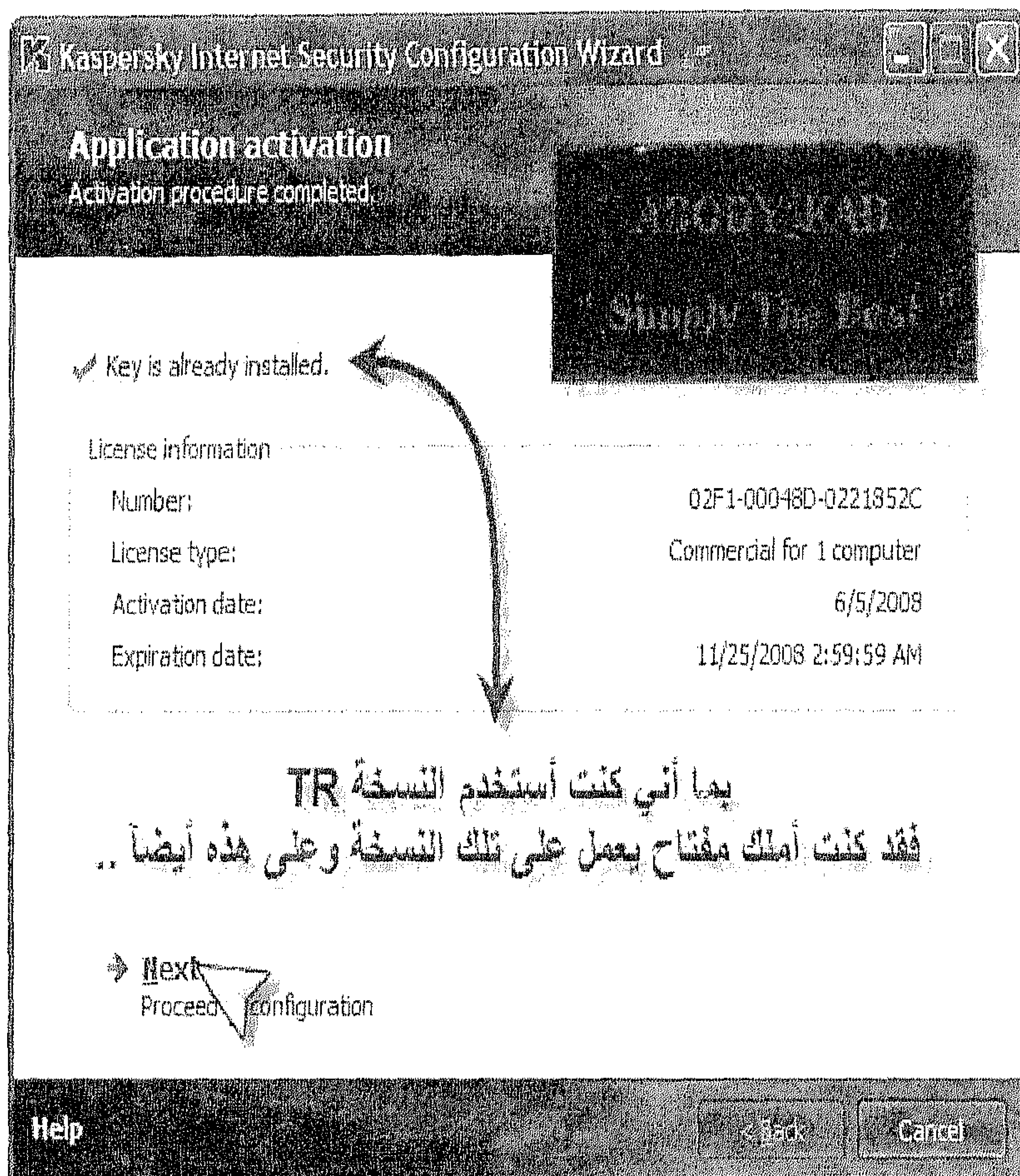
Kaspersky Internet Security 2009
Installation type
Please select the installation type that best suits your needs.
Express installation
Installation with default s[redacted]
Custom installation
Allows users to choose which program features will be installed.
Recommended for advanced users.
Copyright © Kaspersky Lab 1996-2008. All rights reserved.
< Back
Next >
Cancel



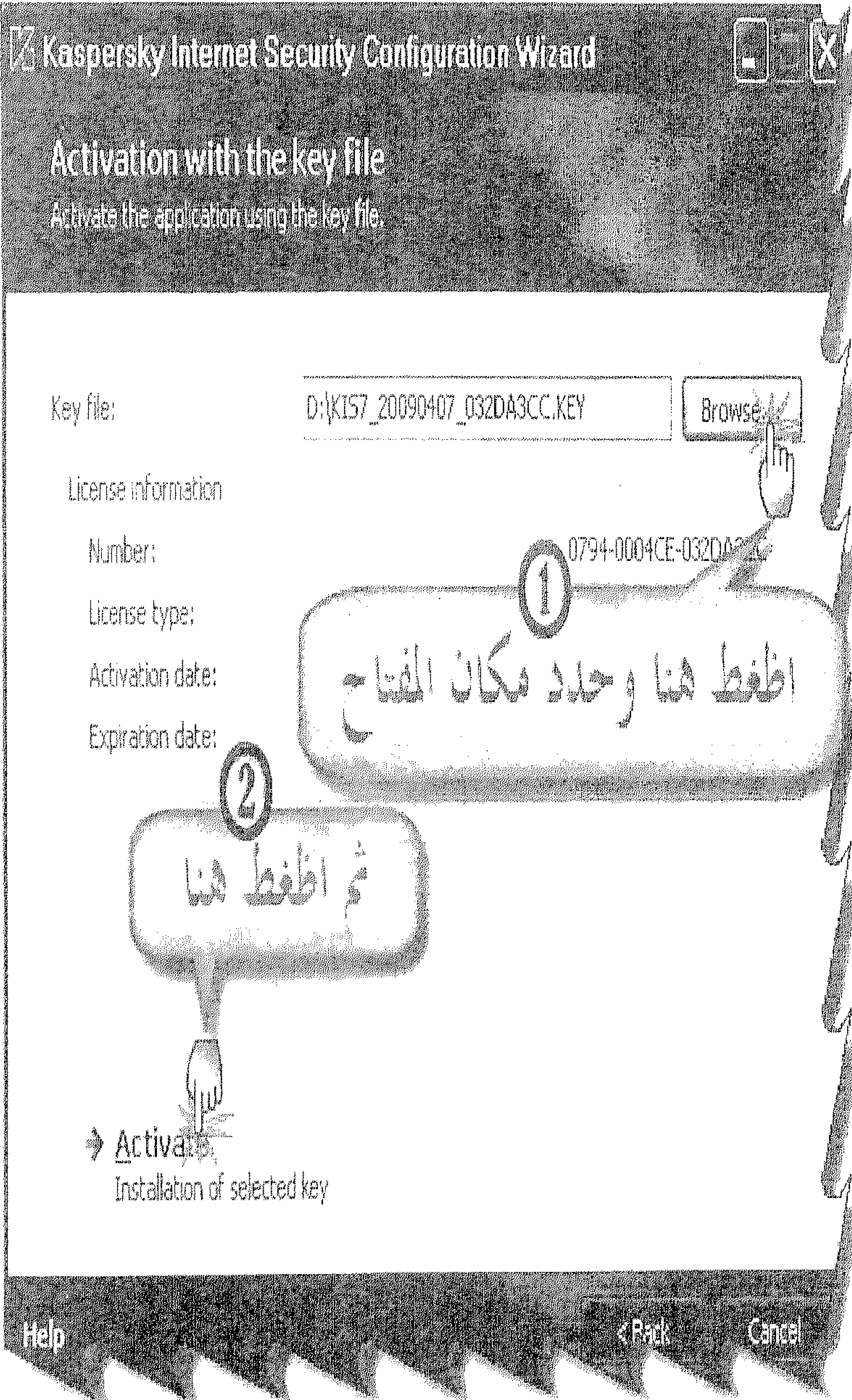
Kaspersky Internet Security 2009
End User License Agreement
Please read the following license agreement carefully.
Please read the license agreement. You must accept the terms of this agreement in order to install the product.
Standard End User License Agreement
NOTICE TO ALL USE[redacted]GAL AGREEMENT
("AGREEMENT"), FO[redacted]ERNET SECURITY
("SOFTWARE") PROD[redacted]AB").
IF YOU HAVE PURCH[redacted] BY CLICKING THE
ACCEPT BUTTON, YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) CONSENT TO
I accept the terms of the license agreement
نوافق طبعاً ..
I do not accept the terms of the license agreement
Copyright © Kaspersky Lab 1996-2008.
< Back
Next >
Cancel

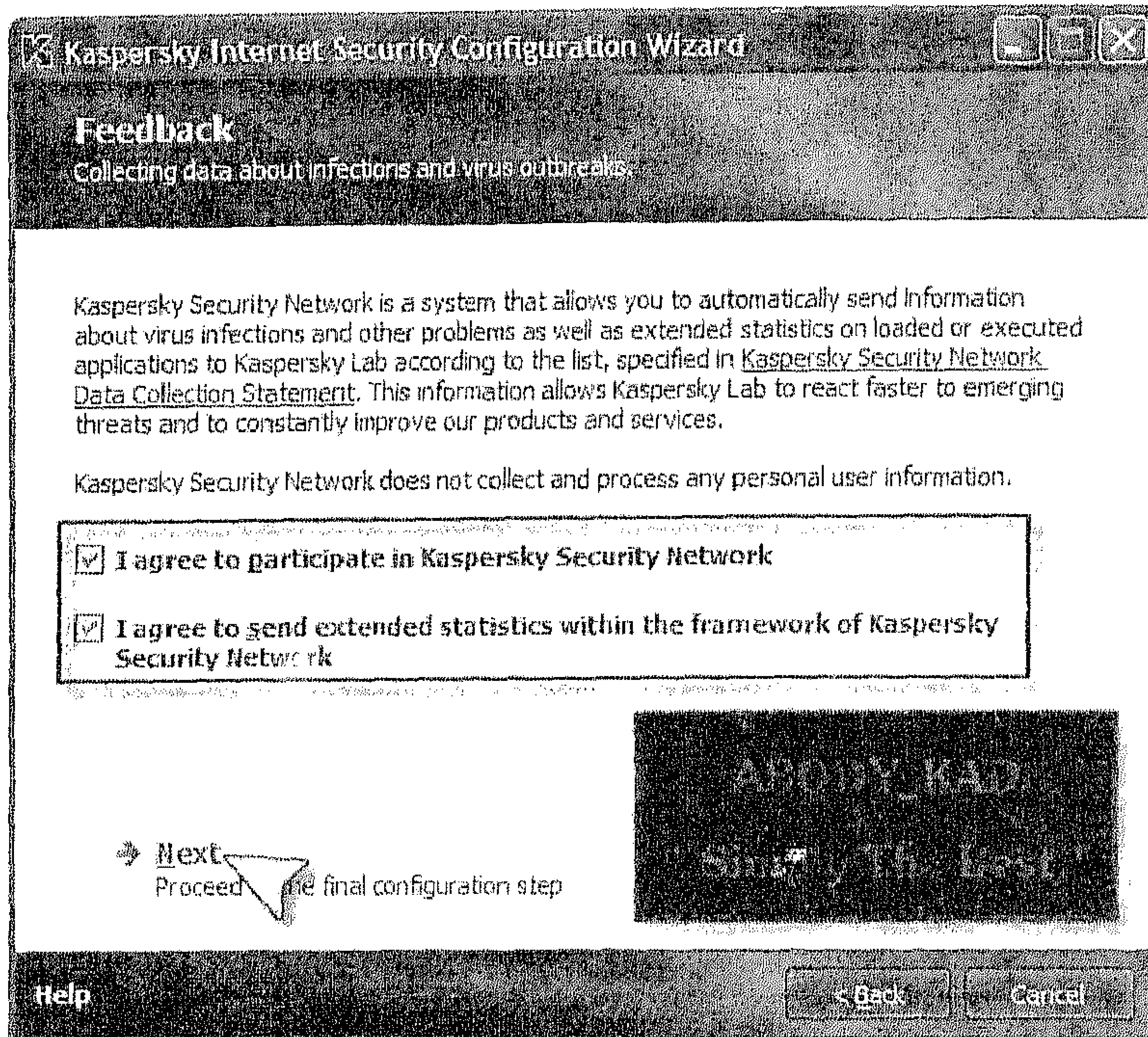

Kaspersky Internet Security 2009
Ready to install
Please confirm that you are ready to install the application.
Click Install to begin the installation. If you want to review or change any of your installation settings, click Back. Click Cancel to exit the Wizard.
Attention! Network or Internet connections can be interrupted and operating system notifications can be displayed during product setup.
< Back
Install
Cancel

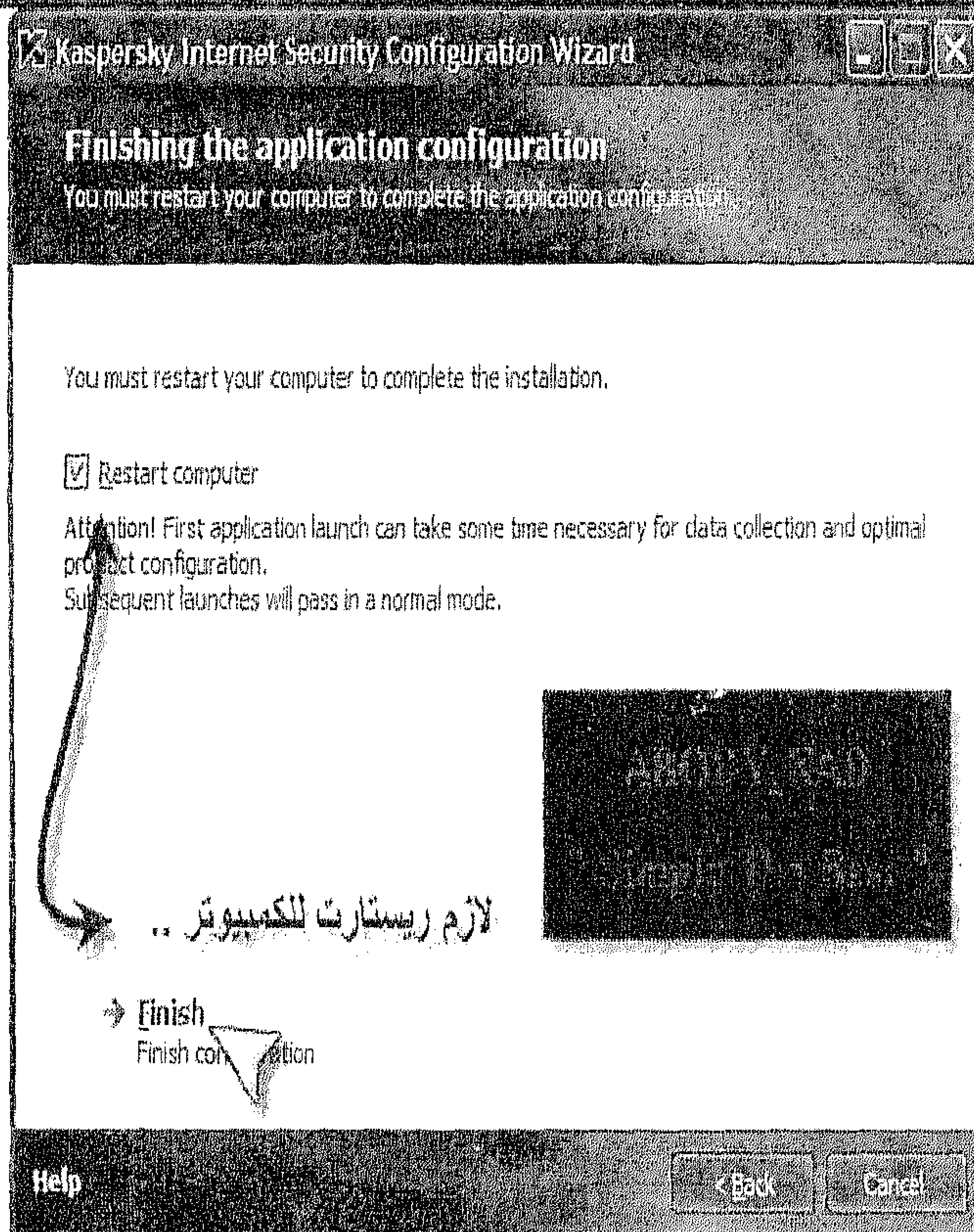

Kaspersky Internet Security 2009
2009
Kaspersky
Internet Security
Installation complete
Setup Wizard has completed successfully. Click Next to start the Application Configuration Wizard.
Next >



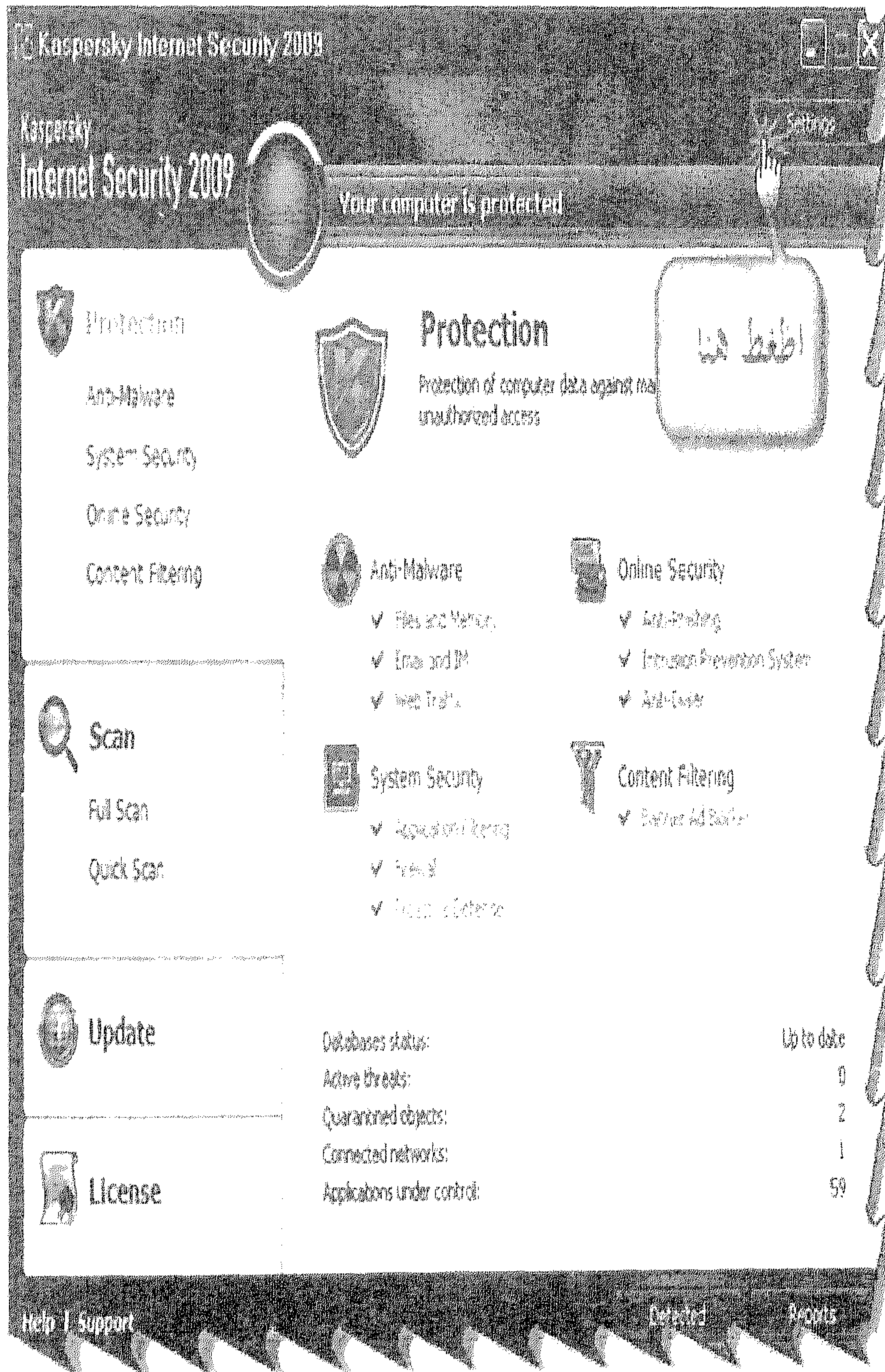
هذه خطوات التفعيل من أخي الكريم الجنتل:

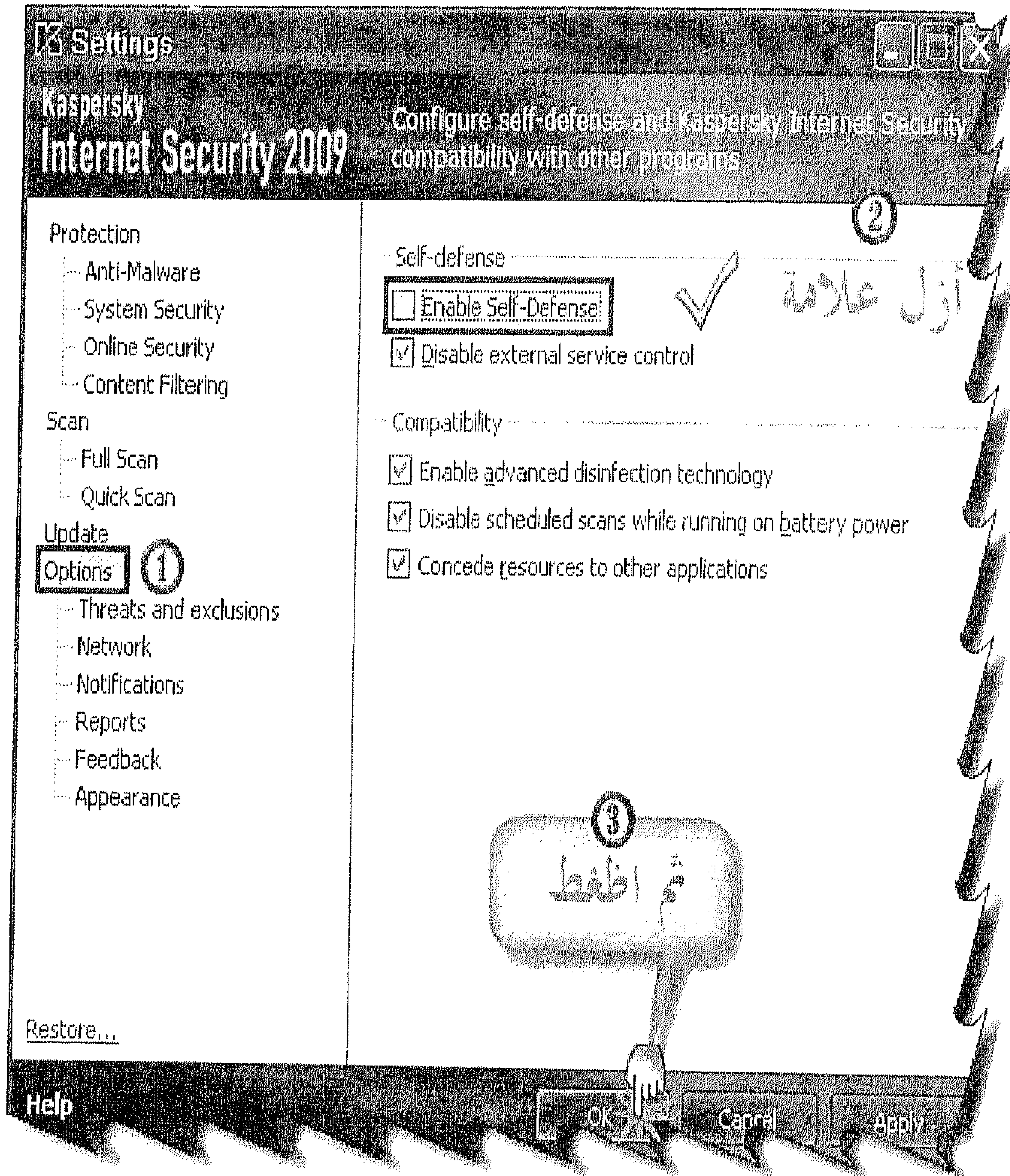

Kaspersky Internet Security Configuration Wizard
Activation with the key file
Activate the application using the key file.
Key file:
D:\KIS7_20090407_032DA3CC.KEY
Browse
License information
Number:
License type:
Activation date:
Expiration date:
اظغط هنا وحدد مكان المفتاح
ثم اظغط هنا
Installation of selected key
Help
Cancel


Kaspersky Internet Security Configuration Wizard
Feedback
Collecting data about infections and virus outbreaks.
Kaspersky Security Network is a system that allows you to automatically send information about virus infections and other problems as well as extended statistics on loaded or executed applications to Kaspersky Lab according to the list, specified in Kaspersky Security Network Data Collection Statement. This information allows Kaspersky Lab to react faster to emerging threats and to constantly improve our products and services.
Kaspersky Security Network does not collect and process any personal user information.
I agree to participate in Kaspersky Security Network
I agree to send extended statistics within the framework of Kaspersky Security Network
Next
final configuration step
Help
< Back
Cancel

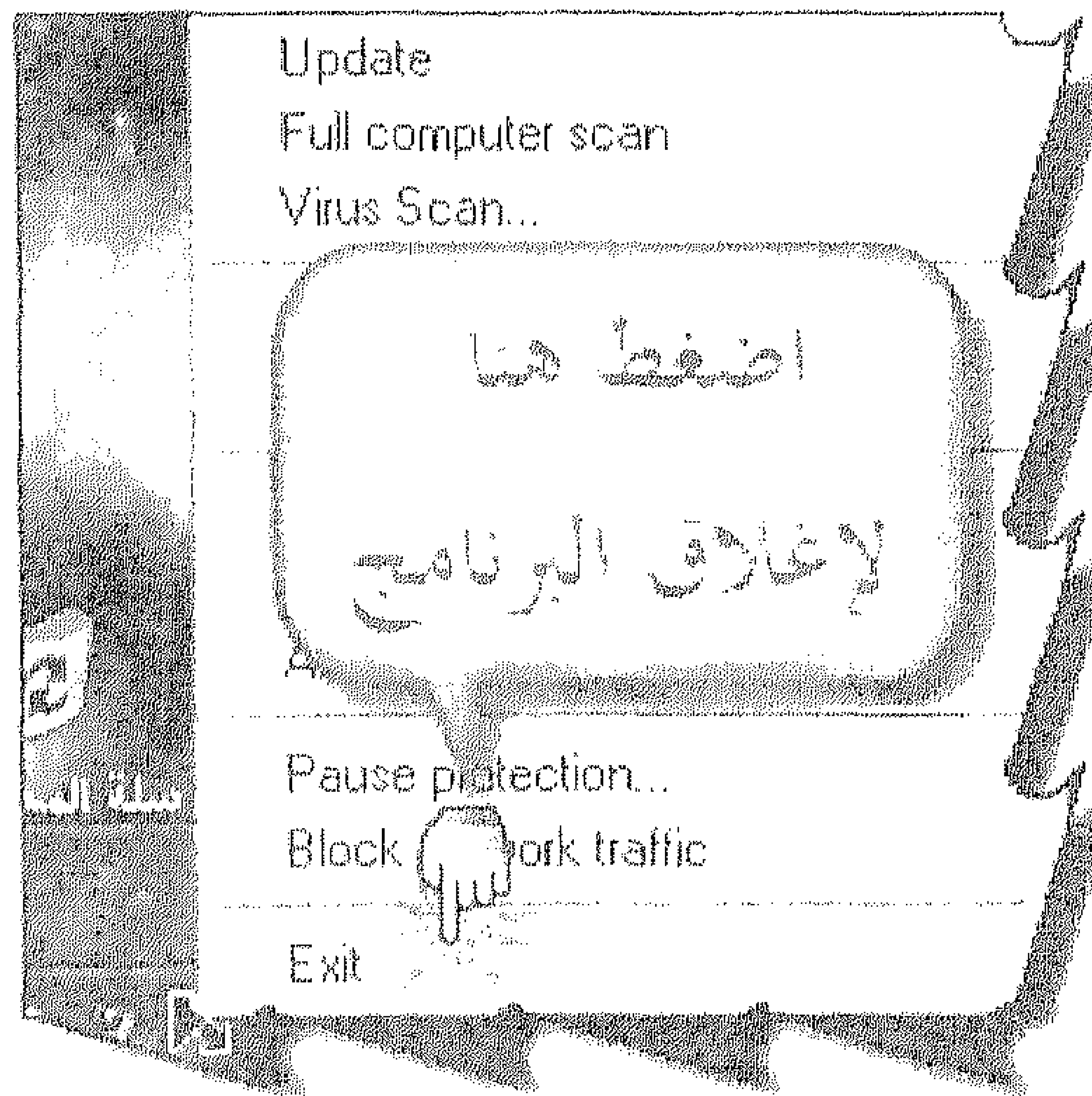

Kaspersky Internet Security Configuration Wizard
Finishing the application configuration
You must restart your computer to complete the application configuration.
You must restart your computer to complete the installation.
Restart computer
First application launch can take some time necessary for data collection and optimal
configuration.
Subsequent launches will pass in a normal mode.
لازم ريستارت للكمبيوتر ..
Finish
Finish
Help
< Back
Cancel

أفتح البرنامج واتبع الصورة

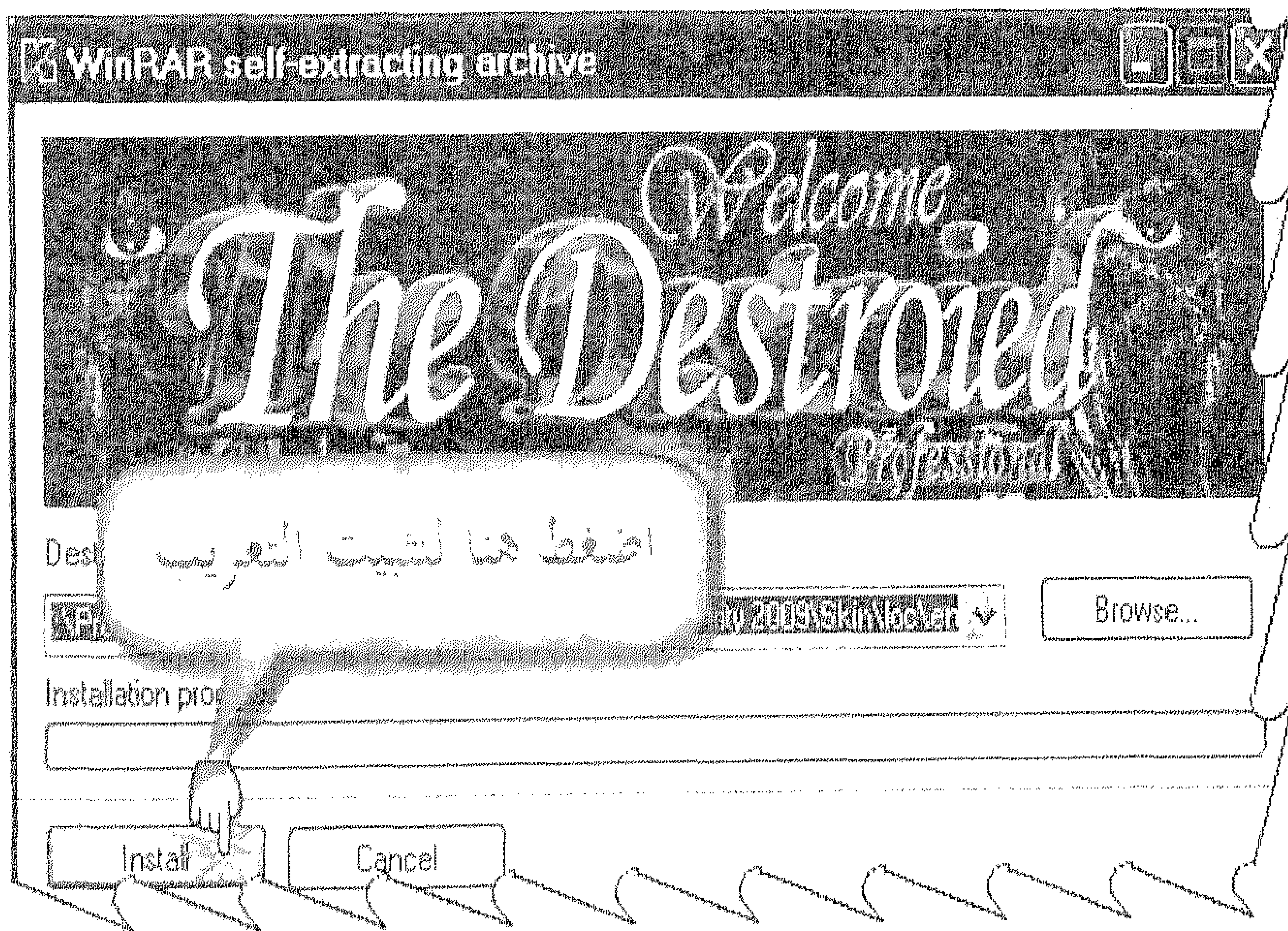




أضغط بزر الماوس الأيمن على شعار البرنامج الذي بقرب الساعة واتبع الصورة

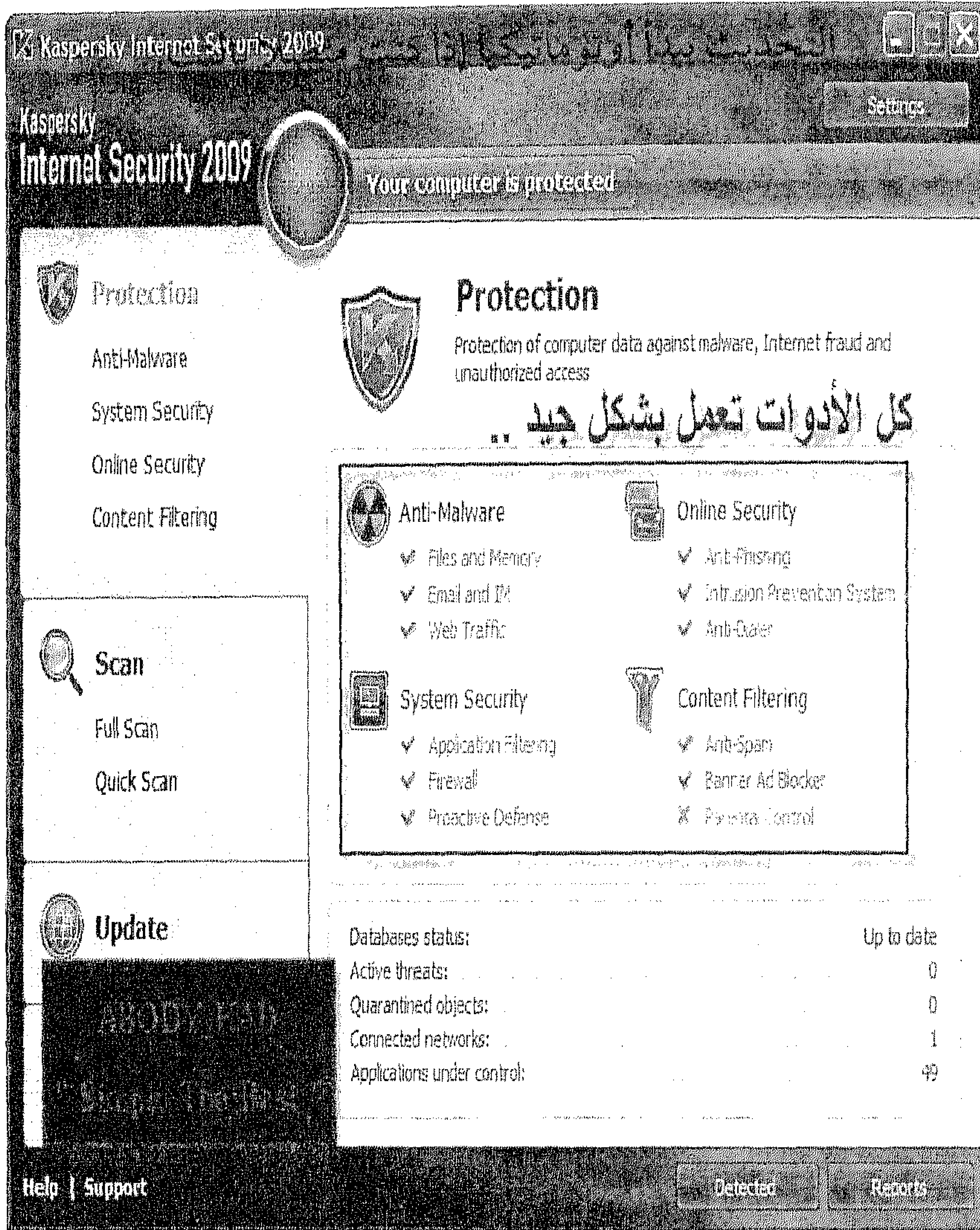


بعد ذلك اضغط على ملف التعريب واتبع الصورة



صور البرنامج

واجهة البرنامج الجديدة والرآئعة:



Kaspersky Internet Security 2009

Settings

Kaspersky
Internet Security 2009

Your computer security is at risk

Fix it now



Protection

Update (3%)

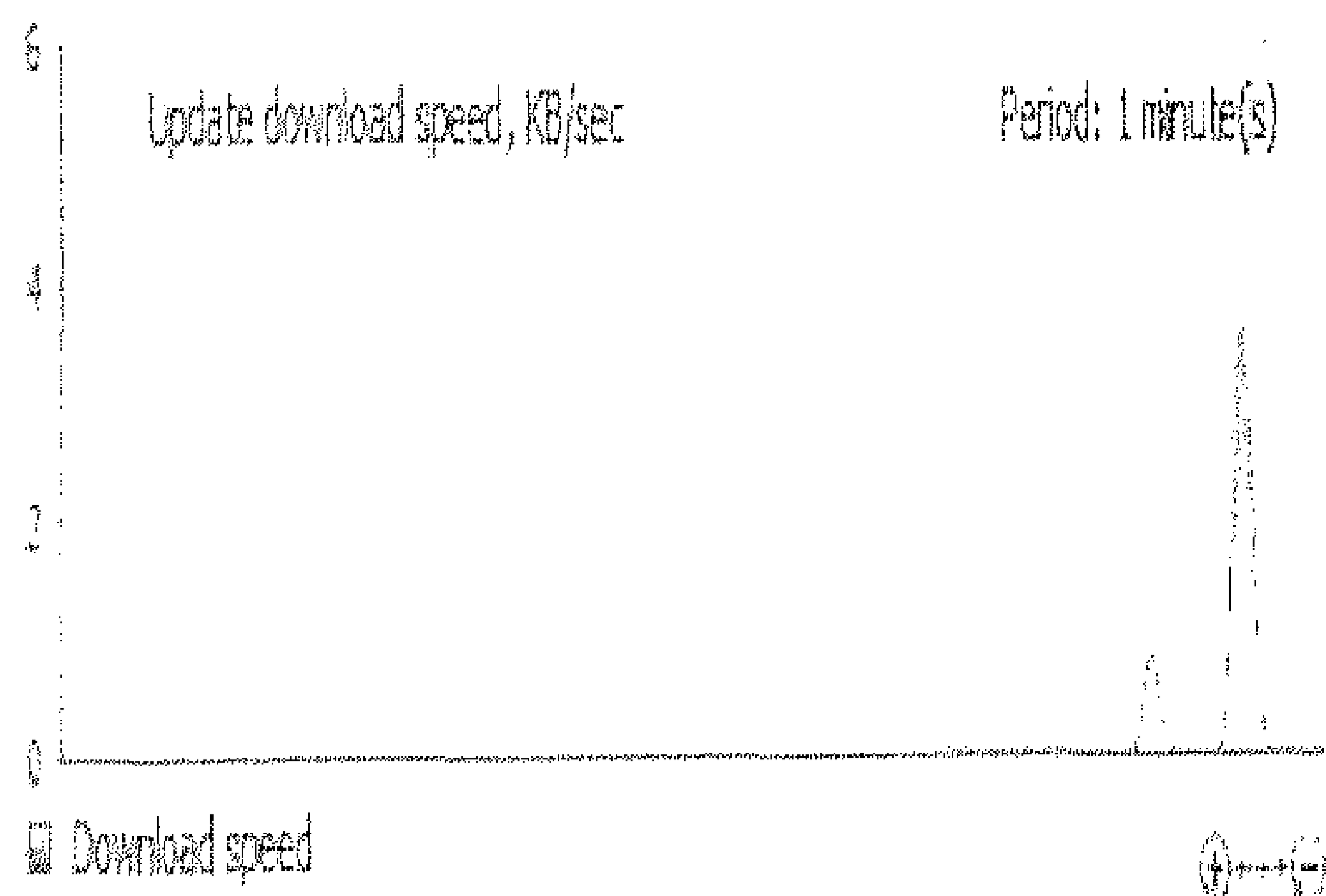
[redacted] databases and program

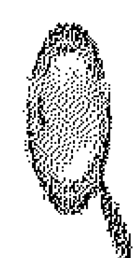
Online Security

Content Filtering

Database status: Obsolete

Virus activity review

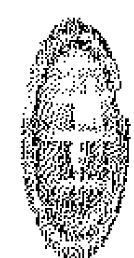




Scan

Full Scan

Quick Scan



Update (3%)

Update size:	4.7 KB
Average speed:	1 KB/sec
Duration:	00:00:23



Stop update



License

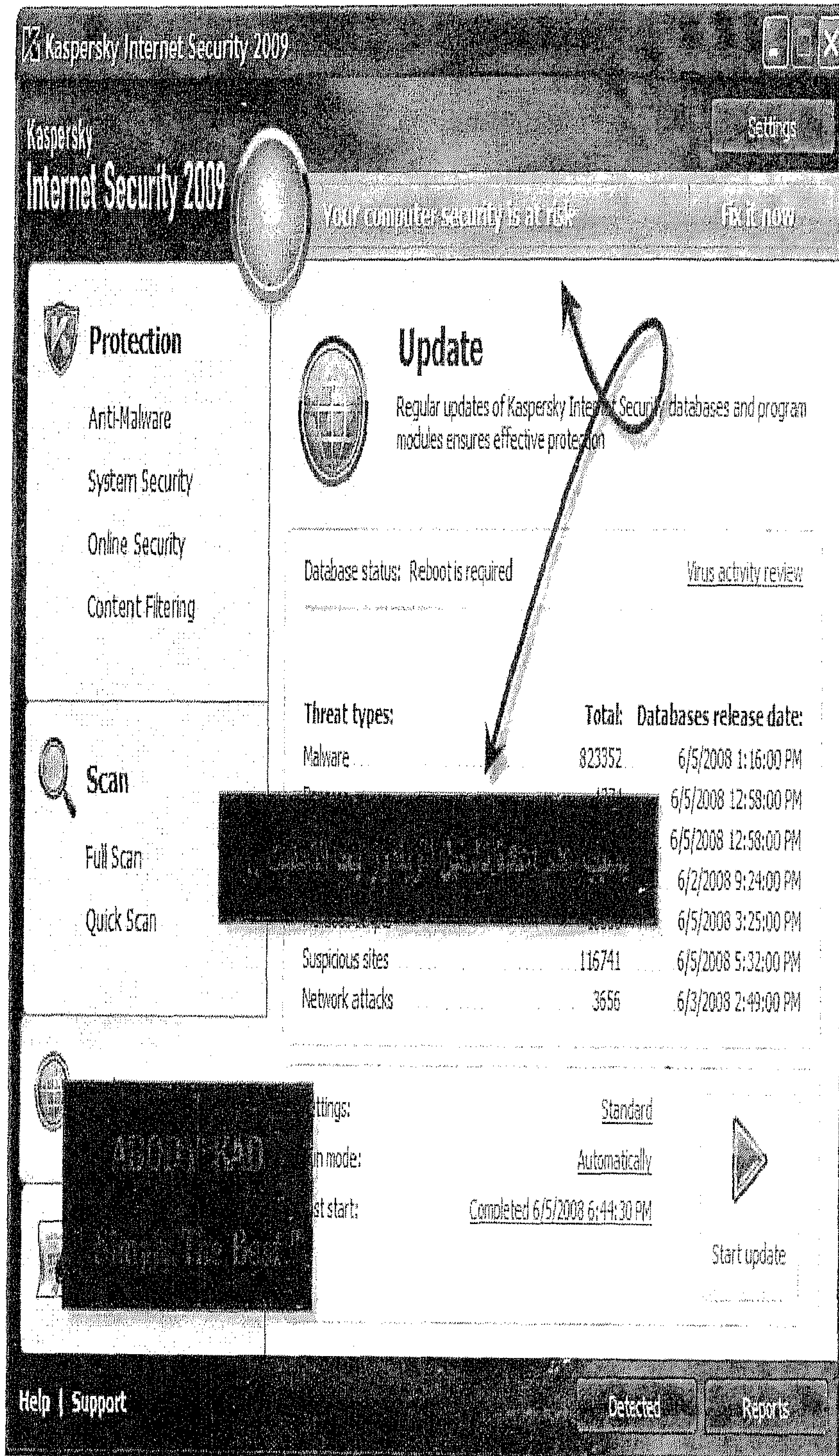
[redacted]

Details

Help | Support

Detected

Reports



النسخة مفعلة و كاملة:

Kaspersky Internet Security 2009



Kaspersky
Internet Security 2009

Settings

Your computer is protected



Protection

Anti-Malware

System Security

Online Security

Content Filtering



Scan

Full Scan

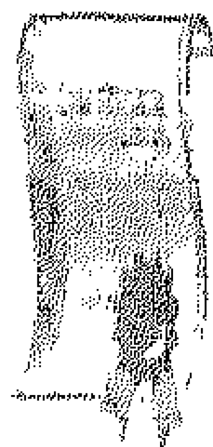
Quick Scan



Update

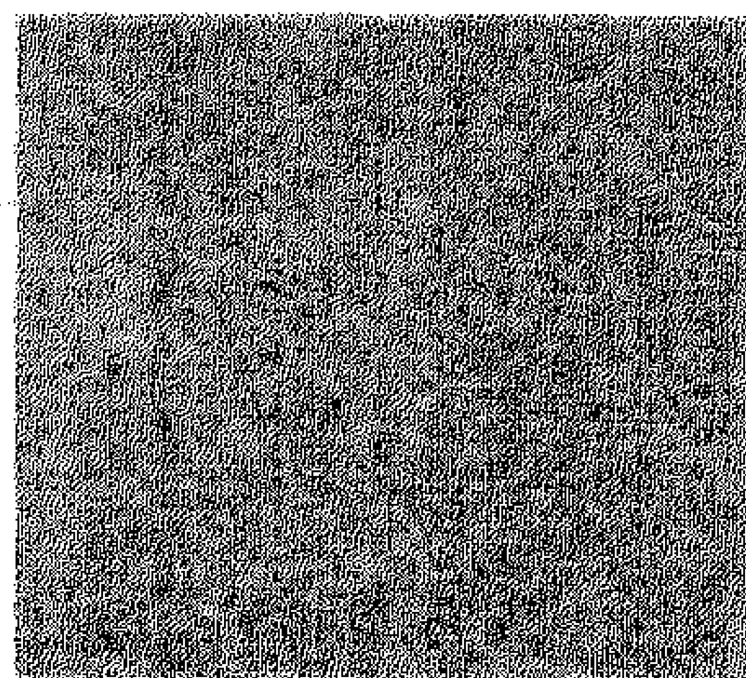


License



License

Protection of computer data against malware, Internet fraud and unauthorized access



License information



Commercial for 1 computer

License validity period expires 11/25/2008 2:59:59 AM

172 days remain(s).



Renew license



Merge/delete



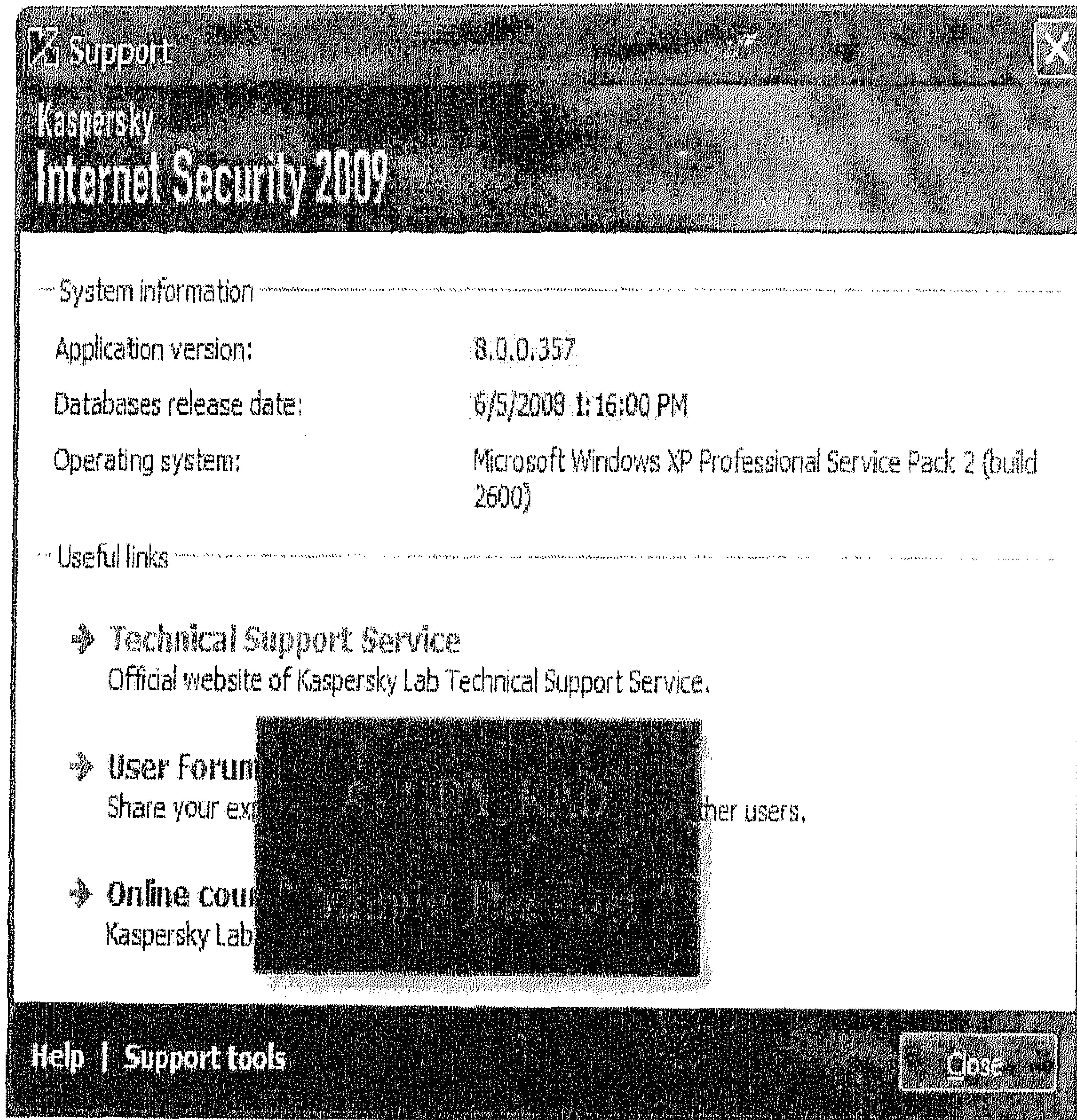
View End User License Agreement

Help | Support

Detected

Reports

نسخة البرنامج:



الوحدة الخامسة

التعرف على الحواجز النارية
Fire Walls
لحماية الشبكة وأجهزتها

المقدمة

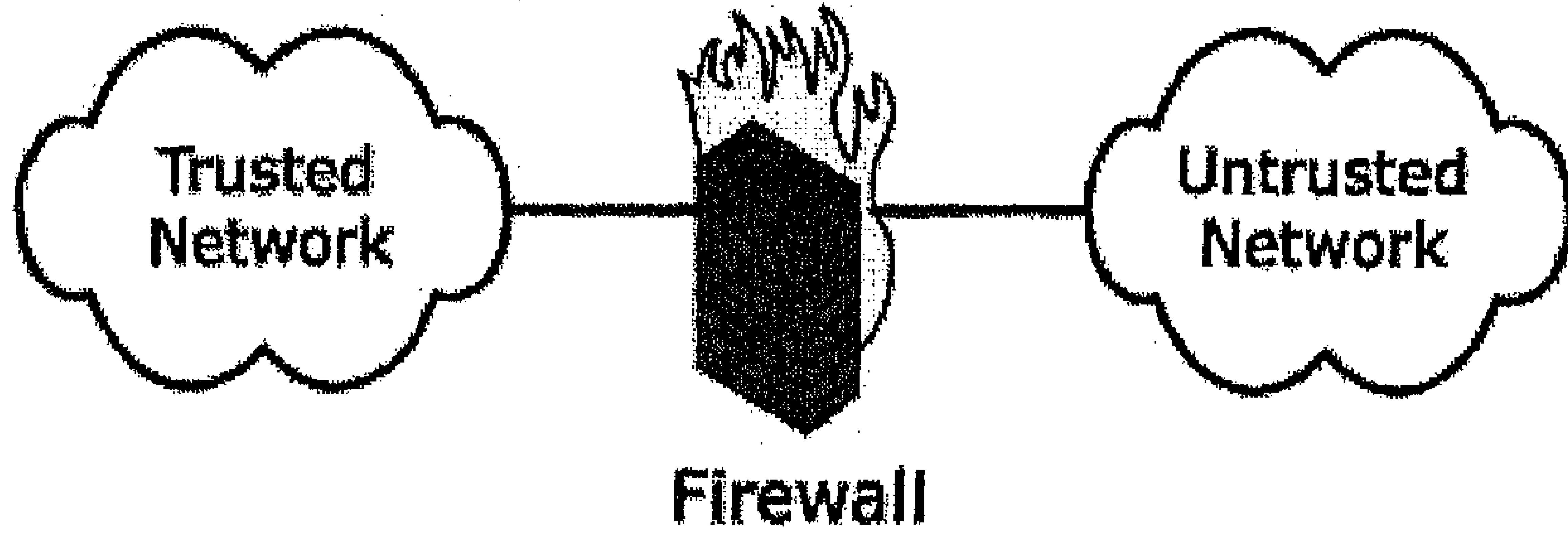
استخدام نظم الحماية المسماة بالجدر النارية Firewalls بأشكاله المتعددة أصبح من الأساسيات في تصميم وتطبيق شبكات الحاسوب على اختلاف أشكالها وأحجامها

هناك الكثير من الأخطار التي تهدد الشبكة الخاصة أو الداخلية .

اتصالات الانترنت التي تتظمنها معظم الشبكات اليوم هي الباب الذي يمكن أن تنفذ منه هذه المخاطر.

١ـ ما هو الجدار الناري Firewall :

– بأنه نظام أو أنظمة معينة هدفها التحكم بانتقال البيانات والوصول للخدمات أو المعلومات بين الشبكات باستخدام قواعد وتعليمات يتم بنائها في نظام الجدار الناري والذي من الممكن أن يكون عبارة عن برنامج software أو كعتاد مادي Hardware.



– في عالم الشبكات فالهدف من الجدار الناري مشابه بشكل كبير للحرائق فالهدف هو إنشاء حاجز بين الشبكة الداخلية (إفتراضا) والشبكة الخارجية وبتعبير أصح عمل حاجز بين الشبكة الموثوقة والشبكة الغير موثوقة بهدف السماح أو منع إنتقال البيانات بين

الشبكتين، ومن أشهر برامج جدران للنار لمستخدمي المنازل Zone alarmمن أقواها.

- كما يمنع جدار الحماية الاتصال المباشر بين شبكة الاتصال وأجهزة الكمبيوتر الخارجية بواسطة توجيه الاتصال عبر ملقم وكيل خارج شبكة الاتصال . يقرر الملقم الوكيل فيما إذا كان مرور ملف ما عبر شبكة الاتصال آمناً. يدعى جدار الحماية أيضاً عبارة الحد الآمن.

- إن جدار حماية اتصال إنترنت Internet Connection Firewall - ICF هو برنامج لتعيين

قيود على نوعية المعلومات المتبادلة بين الشبكة المنزلية.

فإذا كان لديك كمبيوتر مفرد متصل بإنترنت بواسطة مودم الكيبل ، أو مودم DSL ، أو مودم الطلب الهاتفي ، يقوم ICF بحماية اتصالك بالإنترنت.

- الجدار الناري يسمح للمستخدم بإرسال طلباته إلى الإنترنت، ولكنه لا يسمح بالبيانات بالمرور إلى المستخدم من الإنترنت ميزة التنقيح الموجودة في البروكسي يسمح لمسؤولي الشبكة بمنع مرور البيانات من قبل مواقع ممنوعة.

٢- **تأثيرات استخدام الجدار الناري**، وما الذي لا تستطيع الجدر النارية تأمينه ؟

بداية نأتي لذكر التأثيرات الناتجة عن إضافة أحد أنواع الجدر النارية للشبكة ... وهي نوعين تأثيرات إيجابية وتأثيرات سلبية:

٢.١- التأثيرات الإيجابية:

- عند إضافة وتطبيق احد حلول الجدر النارية بطريقة مناسبة ودقيقة فعندها نستطيع التحكم بما يدخل إلى أو وما يخرج من الشبكة التي نريد حمايتها أ بالإمكان منع دخول المتطفلين أو الأشخاص الممنوع دخولهم للشبكة والوصول للموارد الداخلية للشبكة أ بالإضافة للتحكم بالمستخدمين الداخليين للشبكة ومنعهم أو التحكم بوصولهم للشبكات الخارجية مثل بعض خدمات الإنترنت.

٢.١.١- التحقق من المستخدمين user Authentication

بعض الجدر النارية بالإمكان إعدادها بحيث تطلب من المستخدمين اسم المستخدم وكلمة المرور ... بهذه الطريقة يمكن التحكم بنوع الخدمات التي يمكن للمستخدم من الوصول لها بالإضافة لإمكانية تتبع نشاطات المستخدمين.

٢.١.٢-التدقيق والمتابعة

الجدر النارية بالإمكان إعدادها لتسجيل ومتابعة جميع النشاطات والتحركات على الشبكة ... هذه المعلومات المسجلة بالإمكان تخزينها وتحليلها لاحقا بالإضافة لكون أغلب الجدر النارية المزودة بهذه الخاصية توفر العديد من التقارير الواضحة للنشاطات عبر الجهاز.

٢.١.٣- إضافات أمنية أخرى

ليس فقط التحقق والتحكم بالنشاطات عبر الشبكة ولكن أيضا بالإمكان إعداد الجدار الناري ليقوم بإخفاء الشبكة الداخلية عن الشبكة الخارجية ... مثل هذه الإضافة ستوفر الحماية للشبكة الداخلية من عمليات المسح scan الغير مرغوب بها. بالإضافة لإمكانية تشغيل الجدار الناري كنقطة تحكم مركزية لإدارة الشبكة والأمن الإلكتروني.

٢.٢- التأثيرات السلبية:

٢.٢.١- إختناقات الشبكة Bottlenecks

في بعض الإعدادات والتطبيقات للجدر النارية جميع التحركات في الشبكة تلزم بالمرور عبر الجدار الناري أولا مما قد يسبب بازدياد احتمالية حدوث الاختناقات بالشبكة.

٢.٢.٢- تعطل الجدار الناري قد يعطل الشبكة كاملة

في أغلب الحالات الجدار الناري هو نقطة الربط الوحيدة بين الشبكة الداخلية (الموثوقة) والشبكة الخارجية (الغير موثوقة) وبالتالي تعطل الجدار الناري أو حتى في حالة الإعدادات الغير صحيحة سيؤدي لانقطاع الاتصال بين الشبكتين.

٢.٢.٣- مشاكل ناتجة من المستخدمين الداخليين

قد يشعر بعض المستخدمين بالإحباط نتيجة عدم تمكنهم من الوصول لخدمات معينة – الإنترنت مثلا – أو الصعوبة بالنسبة للمستخدم في

حالة تطلب وصوله لخدمة معينة أن يقوم بتأكيد عملية دخوله وحاجته للاحتفاظ بكلمة المرور وغيرها من مشاكل قد تنتج عن المستخدم العادي بعد تطبيق أحد حلول الجدر النارية - الحقيقة مع أنها نقطة قد لا تعتبر كأمر سلبي مباشر عند تطبيق الجدار الناري في الشبكة .. لكن التعامل مع المستخدمين سيشكل نوع من العبء وضياع الوقت بالنسبة لمدير النظام ... بالنسبة لي فقد عانيت مع مستخدمي الشبكة عند تطبيقي للجدار الناري خصوصا موضوع الوصول للإنترنت.

٢.٢.٤ - إضافة عبء ومسؤولية إضافية لمدير الشبكة

بالنسبة لمدير الشبكة قد يضيف الجدار الناري مستوى جديد أو تعقيد اكبر في حالة وجود عطل ما في الشبكة خصوصا عند إهمال أو عدم تتبع رسائل الأخطاء أو تقارير الجدار الناري ... بالإضافة لحاجة مدير النظام للمزيد من الوقت لتتبع أداء الجدار الناري أو قراءة وتتبع التقارير.

٣- أشكال الجدران النارية:

يأخذ برنامج الحماية أحد الشكلين الاثنين :

٣.١- برامج جدر نارية :

برامج مخصصة تعمل على الكمبيوترات الفردية.

٣.٢ - جدر نارية للشبكات:

الة صممت لحماية كمبيوتر أو أكثر.

وكلا النوعين للجدر النارية FireWalls تسمح للمستخدم التعرف على الارتباطات المتجهة للداخل إلى الحاسبات المحمية . والكثير منها أيضا تستطيع القدرة على التحكم في البورتات القادرة أن تصل على الانترنت (من الأجهزة المحمية).

أكثر برامج الحماية وضعت للاستخدام المنزلي (الفردي) وجاءت هذه البرامج بخيارات أمنية يختار منها المستخدم ما يريد ، وكل على حسب رغبته وحاجته.

٤- أنواع الجدار الناري :

1- filter : وهو الذي يقوم بتصفية الدخول والخروج من وإلى الشبكة.

2- proxy : حيث يمتاز بوجود ذاكرة مخبئيه فيه.

3- FILTER&PROXY : حيث يقوم بالوظيفتين السابقتين.

ولكن مهما اختلفت أشكالها ومع تعدد الشركات الصانعة لها فإنها جميعا تعمل بنفس الفكرة والتقنية ، وتقريبا تتساوى في قدراتها في حماية الشبكة، ولكن الاختلاف يكون في طريقة تركيبها وبرمجتها.

٥- أهم تقنيات جدران الحماية :

١- تصفية الحزم (Filter)

٢- ترجمة عناوين الشبكة (NAT)

٣- الملقم الوكيل

٥.١ - تصفية الحزم :

هو النوع الأساسي بين أنواع جدران الحماية ويعمل بطريقة فحص الحزم التي تصل إلى واجهاته ويقرر ما اذا كان سيسمح لها بالوصول إلى الشبكة الأخرى اعتماداً على معلومات يجدها في ترويسات البروتوكولات المستخدمة لبناء الحزم. ويمكن تصفية الحزم على أي طبقة من طبقات OSI المرجعي . ويمكن ان يتسبب في نظام التصفية في إبطاء سرعة الشبكة بشكل ملحوظ . ولابد من تطوير مستمر لجدران الحماية لأن وسائل تتطور للتغلب على التكوينات القياسية لعامل تصفية الحزم.

٥.١.١ - سمات تصفية الحزم :

٥.١.١.١ - العناوين الجهازية (hardware addresses) :

تصفى الحزم على حسب العناوين الجهازية كتمكين كمبيوترات معينة فقط من إرسال البيانات إلى الشبكة الأخرى .ولا يستخدم هذا النوع كثيراً لحماية الشبكات من الوصول إليها بشكل غير شرعي عن طريق الانترنت . ولاكن يمكن استخدام هذا التقنية في جدار حماية داخلي للسماح لكمبيوترات معينة فقط بالوصول إلى جزء معين من الشبكة .

5.1.1.2 - عناوين (IP addresses) :

يمكن استخدام تصفية عناوين IP للسماح فقط للإشارات الموجهة إلى أو الواردة من عناوين معينة بالمرور إلى الشبكة.

٥.١.١.٣- **محددات البروتوكولات** (Protocol Identifiers) :

تستطيع جدران الحماية تصفية الحزم بحسب البروتوكول الذي يحدد المعلومات المحمولة ضمن مخطط IP بياني أمثل بروتوكول التحكم بالنقل (TCP) ، بروتوكول المخططات البيانية للمستخدم (UDP) أو بروتوكول رسائل التحكم بالانترنت (ICMP).

٥.١.١.٤- **أرقام المنافذ** (Port Numbers) :

تستطيع جدران الحماية تصفية الحزم بحسب رقمي منفذي المصدر والوجهة المحددين في ترويسة طبقة النقل ضمن الحزمة .

٥.٢ – ترجمة عناوين الشبكة (NAT) :

وهي تقنية ترجمة عناوين الشبكة وتعمل على طبقة النقل وتحمي كمبيوترات الشبكة من المتطفلين الخارجين عبر الانترنت عن طريق حجب عناوين IP الخاصة بها . وبهذه الطريقة لا يستطيع المستخدمين الخارجيين رؤية الكمبيوترات عن طريق الانترنت . لكن هذا يعني أن أي كمبيوتر على الشبكة لا يستطيع إلا إرسال الإشارات إلى الانترنت لكنه لا يستطيع استلامها .

٥.٣ - الملقمات الوكيلة :

وهي برامج تشبه موجهاتأ (NAT)وتعمل كوسيط بين العملاء على الشبكة الخاصة وبين موارد الإنترنت التي يريدون الوصول إليها وتستطيع الملقمات الوكيلة تخبئة المعلومات التي تصلها من الإنترنتأ بحيث إذا طلب عميل آخر نفس المعلوماتأ يستطيع الملقم الوكيل تقديمها في الحال من مخبأه بدلاً من طلبها ثانية من ملقم الإنترنت . وتستخدم الملقمات الوكيلة لفرض القيود كثيرة على وصول المستخدمين إلى الإنترنت.

٦- كيفية عمل جدار حماية اتصال إنترنت (ICF) Internet Connection Firewall

يراقب جدار الحماية كافة أوجه الاتصالات التي تعبر مساره ويختبر عنوان الوجهة والمصدر لكل رسالة يعالجها. لمنع حركة المرور غير المطلوبة من الطرف العام للاتصال من دخول الطرف الخاص، يحتفظ ICFبجدول لكافة الاتصالات التي تم إجراؤها من كمبيوتر .ICF في حالة الكمبيوتر المفرد، يتتبع ICF حركة المرور الخاصة بالكمبيوتر. عند استخدامه مع ICS ، يتتبع ICF كامل حركة المرور الخاصة بكمبيوتر ICF/ICS والخاصة بأجهزة كمبيوتر شبكة الاتصال الخاصة. تتم مقارنة حركة المرور الواردة من إنترنت مع الإدخالات في

الجدول. ويتم السماح لحركة مرور إنترنت الواردة بالوصول إلى أجهزة الكمبيوتر الموجودة على شبكة الاتصال عند وجود إدخال مطابق في الجدول الذي يظهر بدء تبادل الاتصال من ضمن الكمبيوتر أو شبكة الاتصال الخاصة .

يتم إسقاط الاتصالات الناتجة من مصدر خارج كمبيوترICF ، كإنترنت مثلاً، من قبل جدار الحماية إلا إذا تم إنشاء إدخال في التبويب الخدمات للسماح بالمرور. وعوضاً عن إرسال إعلامات حول النشاط، يقوم ICF بصمت بتجاهل الاتصالات غير المطلوبة، مع إيقاف المحاولات الشائعة للقرصنة مثل مسح المنفذ. إذ أنه يمكن إرسال هذا النوع من الإعلامات بشكل متكرر مما يؤدي إلى تعطيلك عن العمل. عوضاً عن ذلك، يمكن أن يقوم ICF بإنشاء سجل أمان لعرض النشاط المتتبع من قبل جدار الحماية.

يمكن تكوين الخدمات للسماح بإعادة توجيه حركة المرور غير المطلوبة من إنترنت من قبل كمبيوتر ICF إلى شبكة الاتصال الخاصة .على سبيل المثال، إذا كنت تستضيف خدمة ملقم ويبHTTP ، وقمت بتمكين الخدمة HTTP على كمبيوترICF ، فسيتم إعادة توجيه حركة مرور HTTP غير المطلوبة من قبل كمبيوتر ICF إلى ملقم ويب HTTP.تكون مجموعة معلومات العمل والمعروفة بتعريف الخدمة

مطلوبة من قبل ICF للسماح بإعادة توجيه حركة مرور إنترنت غير المطلوبة إلى ملقم ويب على شبكة الاتصال الخاصة.

تستخدم معظم الجهات المعلوماتية الكبرى ومزودو خدمة الانترنت جهاز الجدار الناري FIREWAL بالمكون المادي Hardware إلى جانب الدعم البرمجي Software. إذ يقوم بتزويد المستخدمين بأرقام IP Addressمختلفة تصل إلى عدد خمسين رقم IP داخل الشبكة بينما يتعامل جهاز الجدار الناري مع رقم عنوان IP Address واحد وثابت وهو الذي يتم رؤيته في شبكة الانترنت.

والهدف من تلك الطريقة التوفير بعدد الأرقام وزيادة عدد المستخدمين كما يتم حماية الشبكة وكذلك المستخدمين من خطر الاختراق لكون الرقم الأساسي المستخدم مجهول الهوية بالنسبة للآخرين. ويصعب على المخترقين الوصول أو مجرد معرفة أرقام أجهزة المستخدمين الداخلية.

يمثل تركيب الجدار الناري الخطوة الأولي فقط . في طريق تحقيق امن شبكتك ولا تستطيع غالبا العديد من الجدران النارية التي توظفها الشركات الصغيرة أو متوسطة الحجم منع البرمجيات الخطرة المرسلة في البريد الالكتروني أو أنها تحتاج إلي تكلفة إضافية أو إلي مستوي إضافية من الخدمات الخارجية للقيام بذلك . وتحتاج لكي تشعر بالأمان إلى دراسة شاملة للمواضع المعرضة للهجوم في أنظمة التشغيل والتطبيقات وكلمات المرور والتي تقع خلف جدران النار، كالثغرات الأمنية فيها

بالإضافة إلي الثغرات الكامنة في منافذ الشبكة التي يحميها الجدار الناي ذاته.

وهناك أيضا ما يعرف بنظام الكشف عن الاختراق أو المتطفلين Intrusion Detection System IDS تقوم هذه الأنظمة بالكشف عن أشخاص يتعدون علي الشبكة بالإضافة إلي مهمات أخرى. بما فيها تتبع نشاطات المستخدم منذ دخوله الي خروجه وحراسة الشبكة ضد أنواع معروفة من الهجمات والكشف عن حدوث مخالفات لساسية الشبكة ومتابعة أنشطتها العادية، ما يسهل تحديد أي سلوك غير طبيعي.

٧ـ أكثر الطرق المستخدمة للسيطرة على جهازك الشخصي من قبل المتطفلين :

١- برامج التروجان Trojans.

2- برامج التحكم عن بعد.

3- هجمات رفض الخدمة Denial of service.

4- استخدام خدمات التشارك علي الملفات في بيئة ويندوز من غير وضع كلمة سر.

5- اكواد الهاتف النقال (Java, Java Script, Active X)

٦- رسائل الأيميل المزيفة.

7- تحميل بعض الايميلات على فيروسات.

8-امتداد الملفات المخفية.

٩- مستخدمو برامج المحادثة.

10-التصنت عبر الشبكات المحلية بـSniffer .

٨- مثال على الجدار الناري الخاص بالويندوز XP في طريقة تعامله مع الشبكات :

يتوفر بإصدارة ويندوزXP Professional (الخاصة بالأعمال) جدارا ناريا صلدا من أهم مهامه الأساسية :

١- التخفي Stealth.

2- العمل بقوة في صمت دون مقاطعة المستخدم .

٣- مساندة الشبكات المحلية .

٤- الاستغناء كليا وبمصداقية عن تحميل أي تطبيقات خارجية (جدران نارية) لصد عمليات الاختراق.

٥- سهولة التحميل والتهيئة والعمل في الخلفية دون أدنى تدني لسرعة الجهاز.

٦- التحديث التلقائي ضمن تحديثات ويندوز XP الدورية .

كما يقدم حماية مزدوجة القوة للأجهزة الشخصية المرتبطة بالشبكة وللشبكة ذاتها ، دون التعرض لإتصال الأجهزة الفردية بعضها ببعض عبر الشبكة الداخلية من جانب ، وإتصال الشبكة الداخلية بالإنترنت من جانب أخر .

٨.١- التخفي Stealth :

لمعرفة مصطلح التخفي في الإنترنت علينا أن نتعرف على ميكانيكية المطاردة والصيدChasing & Hunting حيث يقوم المخترق بإرسال رسالة استعلامية مرجعية PING عبر تطبيقات الاختراق ليتسنى له تحديد أرقام الأيبي IPs بالأجهزة ذات المنافذ المفتوحة open portsوهذه دلالة واضحة على أن أصحابها لا يحملون بها جدراناً نارية أو أنهم محملين لجدران نارية إلا أن ملفات تجسسية من نوع أحصنة طروادة Trojans قد تم زراعتها بأجهزتهم بطريقة أو أخرى وقد تمكنت من فتح بعض المنافذ للغزاة . في هذه الحالة نستنتج أمرين ، الأول أن الجدران النارية تقوم بوضع كتل صلدة في وجه رسائل الـ PING، كذلك تغلق المنافذ التي تبحث عن ثغراتها.

٩- ملف تسجيل أمن الجدار الناري :

بعد تنشيط الجدار الناري في الويندوز XP ، لن تجد أية دلاله على وجوده ، فليس هناك ايقونية ظاهرة تدل على وجودة أو اداءة ، بينما هو يعمل بكل طاقته في الخلفية دون أن أي إزعاج للمستخدم ، بل وحتى انك لن تشعر بوجوده ألبته . على كل حال هناك سجل خاص لتسجيل كافة أنشطة محاولات الاختراق وهو الأخر مخفي عن ناظريك ولكنك

حينما تفتح ذلك السجل ستصيبك الدهشة من كفاءة وقوة أداء الجدار الناري الخفي.

٩.١ - تنشيط خيارات سجل الأمان :

تعودنا جميعا عند تحميل الجدران النارية التقليدية مراقبة ايقونية الجدار الناري لملاحظة محاولات الاختراق المضنية ومن ثم متابعة المخترق لتحديد موقعة عبر رقم الأي بي ومعرفة التطبيق الذي يستخدمه للاختراق . ولأننا تعودنا على ذلك فأننا لن نشعر بالاطمئنان في بداية استخدامنا لجدار مايكروسوفت ويندوز XP الناري ، فلا وجود لإيقونات تغمز لإرشادنا لتتبع محاولات الاختراق ، ولا وجود لسجل أمان معين نضغط على أيقونية التطبيق لنفتحه ونشاهد تلك المحاولات. لماذا ؟ ، بكل بساطة لأن الجدار الناري هذا يختلف في طريقة عمله عن بقية الجدران النارية التقليدية ، فليس من مهامة الرئيسية تحديد محاولات الاختراق وكشف التطبيقات التي يستخدمها المخترقون ، بل هو أسمى من أن يتحسس ميكانيكية الاختراق لأن ليس هناك ميكانيكية للاختراق من الأساس حيث انه يخفي جهاز المستخدم Stealth وكأنما هو ليس بمتصل بالانترنت البته ، وعليه فإن محاولات المخترقين تطارد شبحا في هذه الحالة .

على كل حال ، يحتفظ الجدار الناري بسجل خاص لمحاولات الإختراق إن وجدت ولكنه لا يقاطع المستخدم بالتغميز او إصدار لصوت تنبيهي

عند صد كل محاولة للاختراق كما تفعل الجدران النارية التقليدية ، وإنما يعمل في الخلفية دون اية مقاطعة للمستخدم ومتى ما رغب المستخدم في التعرف على سجل محاولات الاختراق للشبح ، فعلية في هذة الحالة فقط الإطلاع على السجل الأمني يدويا وستفاجئه الحقيقة لأنه سيجد السجل فارغا حيث ليس هناك من الأساس صد لمحاولات اختراق لكمبيوتر شبحي.

ملاحظة :

يسمح سجل أمان جدار حماية اتصال إنترنت (ICF) للمستخدمين المتقدمين باختيار المعلومات الواجب تسجيلها .باستخدام تسجيل أمان ICFيمكنك :

١ - تسجيل الحزم المسلّمة. سيسجّل هذا كافة الحزم المسقطة التي تنشأ من شبكة الاتصال المنزلية أو المكتبية الصغيرة أو من إنترنت .

٢ - تسجيل الاتصالات الناجحة. سيسجّل هذا كافة الاتصالات الناجحة التي تنشأ من شبكة الاتصال المنزلية أو المكتبية الصغيرة أو من إنترنت .

٩.١.١ - سجل أمان جدار حماية اتصال إنترنت :

توفر معلومات العنوان معلومات حول إصدار سجل الأمان والحقول المتوفرة لإدخال البيانات. تعرض معلومات العنوان كقائمة ثابتة. إن نص سجل الأمان هو البيانات المترجمة والتي تم إدخالها كنتيجة لمحاولة

حركة المرور عبور جدار الحماية. يتم إدخال الحقول في سجل الأمان من اليسار إلى اليمين عبر الصفحة. إن نص سجل الأمان هو قائمة حيوية، حيث يتم إدخال البيانات عند أسفل السجل. يجب تحديد أحد خياري التسجيل أو كليهما ليتم إدخال البيانات ضمن سجل الأمان .

الجدار الناري في نظام التشغيل windows xp

يعمل على حماية الحاسوب عند اتصاله بالشبكات

اولا امكانيات الجدار الناري :

هي المهام او الوظائف التي يستطيع الجدار الناري ان يؤديها , ومنها :

1. منع البرمجيات غير الموثوقة و غير المرغوب فيها من الوصول الى الحاسوب عبر الشبكة .
2. يطلب الاذن من مستخدم الحاسوب لاتمام اتصال معين او منعه .
3. ينشئ سجلا امنيا بمحاولات الوصول الى الحاسوب من قبل الاخرين (الناجحة وغير الناجحة) مما يساعد في حل المشكلات المستقبلية .

ثانيا : محددات الجدار الناري :
هي المهام او الوظائف التي لا يستطيع الجدار الناري ان يؤديها ومنها:

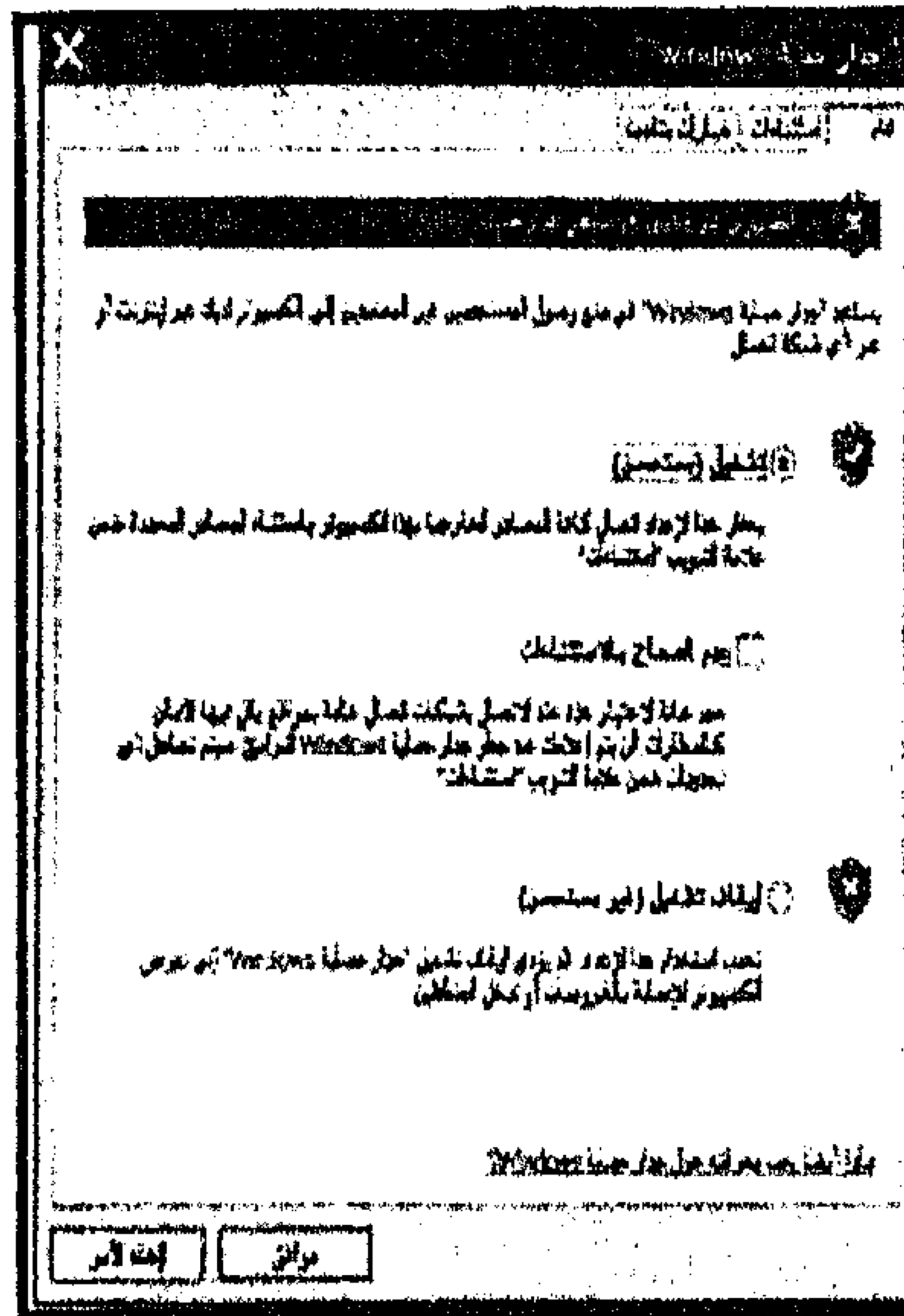
1- كشف الفيروسات او ابطال مفعولها التي دخلت الى حاسوب مسبقا لذا ننصح باستخدام برامج مضادة للفيروسات وتحديثها باستمرار .
2- منع مستخدم الحاسوب من فتح رسالة الكترونيه تحوي مرفقات خطرة لذا ننصح بعدم فتح رسالة الكترونية ومرفقاتها من عناوين مجهولة .
3- منع الرسائل الغير مرغوب بها من الوصول الى البريد الالكتروني .

ثالثا: خطوات اعداد الجدار الناري

- عند اتمام عملية تنصيب نظام التشغيل windows xp فان الجدار الناري يكون تلقائيا في وضع التشغيل . علما انة يمكن ايقافة بشكل كلي او جزئي

اذا اردت التاكد من ان الجدار الناري في وضع التشغيل اتبع الخطوات الاتية :

1- اختر لوحة التحكم control panel من زر ابدا start تظهر لك نافذة لوحة التحكم
2- اختر فئة اتصالات شبكة الاتصال والانترنت لتظهر لك نافذه شبكة الاتصال والانترنت
3- اختر رمز لوحة التحكم جدار الحماية windows يظهر لك صندوق حوار جدار حماية windows firewall



4- لاحظ ان الخيار الفعال هو تشغيل (مستحسن) اغلق صندوق الحوار او النافذه

علل العبارة الاتيه :
لا ينصح بايقاف الجدار الناري في نظام windows xp: لان هذا سيزيد المخاطر الامنية التي يتعرض لها جهاز الحاسوب .

أجهزة الـ:Firewall

تم تطوير الجدار الناري فيما بعد ذلك ليصبح مدمجاً في جهاز إليكتروني يستخدم وبذلك استطاع الجدار الناري مراقبة المستوى الأدنى من الشبكاتTCP/IP

يوجد حالياً العديد من الشركات التي تنتج مثل هذه الأجهزة على سبيل المثال .Cisco - Juniper

تم بعد ذلك إضافة العديد من المزايا لأجهزة الجدار الناري مثل خدمات NAT والـProxy

الوحدة السادسة

التعرف على الملقم الوكيل وخدمات ترجمة بروتوكولات الشبكة

مقدمة

باستخدام الملقم الوكيل يمكنك ربط الشبكة الخاصة أو الشبكة المحلية إلى شبكة عامة مثل الانترنت ، وتعمل بوصفها بوابة للكمبيوتر عميل الداخلية إلى شبكة الانترنت. ملقم وكيل آمنه هو البوابة التي تستطيع استخدامها لتوفير الاتصال بشبكه الانترنت للملكية الفكرية والشبكات القائمة على أساس IPX. بوابة هو جهاز الكمبيوتر الذي يجعل من الممكن لاثنين من شبكات الاتصال.

ملقم وكيل الخدمات يجب أن تدير على جهاز كمبيوتر واحد التي ينتمي إليها كل من الشبكة الخاصة والعامة إلى شبكة مرتبطة.

الكمبيوتر ملقم وكيل إدارة الخدمات ينبغي ان يكون اثنين من وصلات الشبكة :

١. واجهة الشبكة التي تشير إلى الشبكة العامة.

٢. واجهة الشبكة التي تشير الى شبكة خاصة.

عمليات ملقم وكيل تتسم بالشفافية لكمبيوتر عميل. وهذا يعني ان المستخدمين لا يدركون أن ملقم وكيل الطالبة فعلا على الانترنت نيابة عنهم. المستخدمون ألا يصبح على بينة من وجود الملقم الوكيل عندما طلب ان محتوى ملقم وكيل وقد جرى تشكيله لأرفض. ملقم الويب خدمة طلب للمحتوى هذه الطلبات العمليات كما لو أنها نابعة من

المستخدمين الفعلية.

ملقم وكيل مايكروسوفت الإصدار ٢،٠ هو امتداد جدار الحماية ومضمون مخبأ الخادم. ملقم وكيل الإصدار ٢،٠ الآمن ينص على شبكة الانترنت ، وزيادة سرعة الوصول الى شبكة الانترنت ، وخدمات التخزين المؤقت لشبكة يحسن وقت الاستجابة. ملقم وكيل يمكن محليا مخبأ مواقع الانترنت والملفات التي كثيرا ما طلب منها ذلك. بعد ذلك تطلب هذه الخدمات من ذاكرة التخزين المؤقت المحلية. وهذا يؤدي إلى زيادة في أداء الانترنت. ملقم وكيل يمكن أن توفر شبكة معالجة الترجمة لدعم القطاع الخاص لمعالجة الملكية الفكرية. ملقم وكيل وتشمل عددا من الخدمات التي يمكن للمشرفين على إدارة واستخدام التحكم في الاتصالات الى شبكة الانترنت. يمكنك الحد من المواقع التي يمكن للمستخدمين الوصول. يمكنك أيضا منع غير مأذون به لمستخدمي الانترنت من الوصول إلى الشبكة الخاصة.

ملقم وكيل وعندما تستخدم مدخلا إلى الانترنت ، دون إذن مستخدمي شبكة الانترنت في الأساس إلى منعهم من الوصول الى الشبكة الخاصة. ويرجع ذلك إلى ملقم وكيل ويجري الجدار الفاصل بين القطاع الخاص وشبكة شبكة عامة -- طلبات المحتوي على شبكة الانترنت يسمح ، ودخول غير مصرح به من شبكة الانترنت هو

طريق مسدود. ولكن يمكنك استخدام ميزة عكس بالوكالة لمستخدمي شبكة الانترنت مع توفير القدرة على الوصول الى المواقع على شبكة الانترنت على الشبكه عبر ملقم وكيل.

١ - إستخدام عنوان الإنترنت IP للمصدر في اتخاذ قرارات التوجيه :

يعتبر استخدام عنوان الإنترنت IP للمصدر في اتخاذ قرارات التوجيه آليّةً ملائمةً لتوزيع الحمل Load Balancing في الشبكات اللاسلكية. يمكننا باستخدام موجّهٍ قادرٍ على اتخاذ القرارات بناءً على عنوان مصدر الحزم تطبيق مستوياتٍ مختلفةٍ من جودة الخدمة Quality of Service للحواسب المختلفة، كما يمكننا أيضاً توجيه مستخدمين مختلفين للشبكة اللاسلكية إلى موجّهاتٍ طرفيّةٍ Border Routers مختلفة.

لا يتطلّب استخدام التوجيه المسيّس بناءٍ على عنوان المصدر Source IP على سبيل المثال تغيير عنونة الشبكة اللاسلكية لتوصيل مستخدمٍ معيّنٍ إلى بوابةٍ خارجيّةٍ مختلفةٍ عن تلك المستخدمة من قبل الآخرين.

٢ـ الملقم الوكيل ترجمة عناوين الشبكة Network Address Translation (NAT):

يعتمد مبدأ ترجمة عناوين الشبكة NAT على قدرة الموجّه على "إعادة كتابة" عنوان الوجهة أو المصدر لحزم بروتوكول الإنترنت IP. لقد

انتشرت ترجمة عناوين الشبكة NAT على نطاقٍ واسعٍ لأنّها تتيح لجهازٍ واحدٍ يملك عنوان إنترنت عام Public IP أن يقوم بتمثيل مجموعةٍ من الحواسب ضمن شبكةٍ خاصّةٍ.

٢,١ـ خصائص ترجمة عناوين الشبكة NAT :

تم تصميم NAT لتوفير(عدم هدر) عناوين IP وتمكين الشبكات ذات العناوين الخاصة من الوصول إلى الانترنت .

يتم ذلك عبر ترجمة العناوين الخاصة الداخلية ضمن الشبكة إلى عناوين عامة يمكن استخدامها ضمن الانترنتأ وهذا باختصار عمل NAT.

يقوم NAT بتغيير العناوين داخل حزمة البيانات Packet.

إن عملية الترجمة هذه يمكن أن تتم بشكل ديناميكي متغير أو بشكل ثابت.

ولعل الميزة المهمة التي تزيد من قدرات NAT هي ترجمة المنافذ أو ما يسمى PAT والتي تتيح استخدام عنوان وحيد عام لخدمة الشبكة ذات العناوين الخاصة،عادة ما يسمى PAT باسم : NAT ذو علاقة (الجميع إلى واحد).

٢,٢ـ أنواع الملقم الوكيل عناوين NAT :

٢,٢,١ـ عناوين NAT الثابتة :

فهي مصممة بشكل يسمح بتعيين العناوين العامة والمحلية من عنوان إلى آخر بنمط واحد لواحدأ يعد ذلك مفيدًا بصفة خاصة للمضيفين الذين يجب أن يكون لهم عنوان ثابت يمكن الوصول إليه من الإنترنت.

٢.٢.٢- عناوين NAT الديناميكية : تستخدم لتعيين عنوان IP خاص إلى عنوان عام. ويتم تعيين أي عنوان IP من تجميع عناوين IP العامة إلى مضيف شبكة .

لا تقتصر أهميّة ترجمة عناوين الشبكة NAT على تجاوز مشاكل شح عناوين الإنترنت الحقيقيّة Public IP Addresses بل تكمن أيضاً في اعتمادها كآليّةٍ لتطبيق مهام الشبكة التالية :

٣ـ مهام ترجمة عناوين الشبكة (NAT) :

١- الجدار الناري Firewall / المنطقة منزوعة السلاح DMZ.

٢- توزيع حمل حركة البيانات Traffic Load Balance (مثال: مجموعة من مخدّمات الوب المتماثلة خلف خدمة NAT لتوزيع طلبات الوصول إلى مواقع الإنترنت).

٣- توزيع حمل معالجة البيانات Computing Load Balancing (مثال: مجموعة من قواعد البيانات المتماثلة لتوزيع حمل معالجة طلبات الوصول إلى البيانات).

٤- مزايا ترجمة عناوين الشبكة (NAT) :

إلغاء عملية إعادة تعيين عنوان IP جديد لكل مضيف عند التغيير إلى ISP (موفر خدمة الإنترنت) جديد. حيث يقوم بروتوكول NAT بإلغاء الحاجة إلى إعادة عنونة كل المضيفين الذين يتطلبون وصولاً خارجياً، مما يؤدي إلى توفير الوقت والمال.

باستخدام PAT، يتمكن المضيفون الداخليون من مشاركة عنوان IP عام واحد في جميع الاتصالات الخارجية. وفي هذا النوع من التكوين، يلزم وجود عدد قليل جدًا من العناوين الخارجية لدعم العديد من المضيفين الداخليين، وبذلك يتم توفير(عدم هدر) عناوين IP.

زيادة أمن الشبكة نظرا لأن الشبكات الخاصة لا تعلن عن عناوينها أو هيكلها الداخلي، فإنها تظل آمنة بشكل معقول عند استخدامها مع NAT للحصول على وصول خارجي خاضع للتحكم.

استخدام ترجمة عناوين الإنترنت NAT لتحسين أمن الشبكة.

٥- الفوائد الرئيسية وسمات ملقم الوكيل :

الملقم الوكيل يقوم بتأمين توفر مدخلا الى شبكة الانترنت. انه بمثابة نقطة مراقبة بين القطاع الخاص وشبكة الانترنت. ويمكنك ايضا للتحكم في تدفق حركة المرور في ملقم وكيل.

ونظرا للملقم وكيل اثنين من بطاقات واجهة الشبكة ، والشبكة المحلية مؤمن من غير المرخص لهم محاولة للوصول إلى الشبكة الخاصة. نقطة واحدة فقط من وجود اتصال بين القطاع الخاص وشبكة الانترنت.

ملقم وكيل ويشمل أيضا دعم نشر على الشبكة العالمية. يمكنك الاستفادة من ميزة عكس بالوكالة لمستخدمي شبكة الانترنت مع توفير القدرة على الوصول إلى خدمة ويب استضافت على الشبكة من خلال

ملقم وكيل. العكس يحدث عندما تستضيف خدمة ويب متعددة قادرة على أن تنشر على شبكة الانترنت.

يمكنك الحد من المواقع التي يمكن للمستخدمين الوصول إليها.

استخدام الانترنت لكل مستخدم يمكن تعقبها وتسجيلها.

٦- الطريقة الأولى \ إعدادات الملقم الوكيل لمتصفح الإنترنت إكسبلورر عند إستخدام النطاق العريض أو / و شبكة المنطقة المحلية اتصال الإنترنت :

إبدأ تشغيل متصفح الإنترنت إكسبلورر Internet Explorer - من الأيقونة الموجودة على سطح المكتب بالنقر عليها لمرتين بزر يسار الفأرة .

إختر أدوات ← Tools - خيارات إنترنت Internet Options - ...من القائمة الرئيسية المنسدلة .

ستفتح نافذة أخرى فيها عدة خيارات إنتقل إلى صفحة الاتصالات - Connections.

انقر على رز إعدادات الشبكة المحلية . LAN Settings -

تحقق من خيار استخدم ملقم وكيل لشبكة المنطقة المحلية الخاصة بك - Use a proxy server for your LAN

أكتب local host في حقل العنوان) Address -كبديل لذلك ، يمكنك أن تدخل عنوان المعرف الرقمي لجهاز الحاسب المتصل (الآي بي127.0.0.1 (، وهو نفس ما هو موجود في .(local host)

أدخل الرقم12080 في خانة المنفذ Port.

أكد عمليتك بالنقر على زر OK.

٦ – الطريقة الثانية \ إعدادات الملقم الوكيل لمتصفح الإنترنت إكسبلورر عند إستخدام استخدام الإتصال العادي (مودم دايل- أب) للإتصال بالإنترنت

إبدأ تشغيل متصفح الإنترنت إكسبلورر Internet Explorer – من الأيقونة الموجودة على سطح المكتب بالنقر عليها لمرتين بزر يسار الفأرة .

إختر أدوات ← Tools – خيارات إنترنت Internet Options - ...من القائمة الرئيسية المنسدلة .

ستفتح نافذة أخرى فيها عدة خيارات إنتقل إلى صفحة الاتصالات – Connections.

إختر إتصالك العادي المعد سابقاً (دايل – أب) من القائمة و إنقر على رز إعدادات . Settings -

تحقق من خيار استخدم الملقم الوكيل لهذا الإتصال Use a proxy - server for this connection.

أكتبlocal host في حقل العنوان Address –كبديل لذلك ،

يمكنك أن تدخل عنوان المعرف الرقمي لجهاز الحاسب المتصل

(127.0.0.1)، وهو نفس ما هو موجود في (local host)

أدخل الرقم12080 في خانة المنفذ Port .

أكد عمليتك بالنقر على زر OK .

مقدمة في أمن الشبكات

Net Work Security





دار المعتز للنشر والتوزيع
عمان - وسط البلد - مجمع الفحيص التجاري
تلفاكس: ٤٦٢٠٩٩٠ ٦ ٩٦٢+ ص.ب: ١٨٤٠٣٤ عمان: ١١١١٨ الأردن
e-mail:daralmuotaz@yahoo.com